UNIVERSIDADE FEDERAL DE PERNAMBUCO
DEPARTAMENTO DE MATEMÁTICA

Aritmética das Curvas de gênero 0 e 1 sobre os corpos $\mathbb{F}_q$ e $\mathbb{Q}$

Ricardo Pereira da Conceição
Recife, Janeiro de 2003

Agradecimentos

Agradeço a Deus, cuja sabedoria e amor têm sido de fundamental importância nestes meus anos de vida.

Agradeço também as seguintes pessoas que direta ou indiretamente contribuíram nesta fase de minha vida. No âmbito acadêmico agradeço:

- Ao prof. Francesco Russo, pela orientação precisa, pelo empenho, dedicação, paciência, conselhos, sabedoria e amizade: as qualidades de um verdadeiro "Conselheiro";
- Ao professor Israel Vainsencher, sempre atencioso e incentivador;
- A Arnaldo Garcia, por fazer parte da banca;
- A Marc Hindry, pela motivação e experiência transmitida em seu excelente curso na Escola de Álgebra;
- Aos meus primeiros mestres na matemática, os meus queridos professores da UEFS, a quem devo todo o incentivo inicial: Hildete, Haroldo, Carloman e João Cardeal;
- As funcionárias Tânia (UFPE) e Andiara (UEFS), pela dedicação, pela paciência, empenho;
- A Capes, pelo suporte financeiro.

No âmbito pessoal, serei eternamente grato:

- Aos meus familiares: minha mãe, minha estrada e minha luz, cuja presença constante em meus pensamentos é sempre um motivo para prosseguir; a minha

vó, minha outra mãe, cuja força e valores são minhas maiores heranças; aos meus tios pelo inestimável apoio e confiança que depositaram em mim; ao meu irmão, que me deu muitas alegrias e sobrinhos lindos; as tias e primos;

- Renata, cujo sacrifício, carinho, dedicação, paciência e organização tem sido constantes: Longos são os dias sem tua presença;
- Aos amigos conquistados e que me conquistaram, o suporte espiritual necessário para o término deste trabalho;
- Em especial aos amigos Adson, Ana Cristina e Taíse, vocês não imaginam a importância de vocês em minha vida.

Conteúdo

Introdução

A Teoria dos Números é a parte da Matemática que se interessa pelas propriedades dos números inteiros e racionais e desde muito tempo atrás matemáticos de diversas eras têm se debruçado sobre seus segredos: foi assim com Euclides, que dedicou alguns volumes de seus "*Elementos*" a ela, e assim tem sido, já que atualmente o interesse nesta área renova-se a cada dia.

Fermat foi um dos maiores expoentes da Aritmética. Foi ele quem propôs o mais famoso problema da matemática, a conjectura que mais possuiu demonstrações erradas, o resultado mais perseguido por amadores e matemáticos, o teorema que muito fertilizou o solo do conhecimento matemático e que também revelou relações inesperadas entre as várias partes da matemática, o teorema cuja demonstração, tão desejada, mostrou-se distinta de tudo aquilo que já se imaginou, o resultado que deu origem a este trabalho.

O teorema que Fermat propôs, hoje conhecido como o *O Último Teorema de Fermat* ou o *Grande teorema de Fermat*, pertence a um campo da matemática que estuda as *equações diofantinas*, isto é, as soluções inteiras ou racionais de equações algébricas de uma ou mais variáveis sobre $\mathbb{Z}$ ou $\mathbb{Q}$. Mesmo estando a Teoria dos Números preocupada com as soluções inteiras, ela utiliza-se de todas as ferramentas da Matemática para obter seus resultados, e, no caso das equações diofantinas, já está mais do que comprovado que as técnicas da geometria algébrica são de inestimável importância; tanto que muitos resultados importantes só puderam ser obtidos mediante um misto de técnicas geométricas e aritméticas. Por exemplo as soluções em R, R domínio de integridade, de uma equação algébrica em n variáveis com coeficientes no anel $L \subseteq R$ se interpretam como os pontos com coordenadas em R da correspondente hipersuperfície em $R^n = \mathbb{A}^n_R$. Esta área mista é hoje amplamente conhecida por *Geometria Diofantina* ou para corpos mais gerais *Geometria Aritmética*.

Este trabalho visa estudar os primeiros problemas da Geometria Aritmética: as curvas lisas de genêro 0 e 1 sobre os corpos $\mathbb{F}_q$ e $\mathbb{Q}$.

No primeiro capítulo são recolhidos os preliminares da teoria das curvas algébricas lisas definidas sobre um corpo K e os principais teoremas e resultados que serão utilizados na continuação da tese.

As curvas de genêro 0 são tratadas no 2^o capítulo, onde mostramos que toda curva lisa de genêro 0 definida sobre um corpo qualquer K é isomorfa a $\mathbb{P}^1_K$ ou a uma cônica definida sobre K. Estudamos em detalhe a geometria das cônicas sobre um corpo qualquer de característica diferente de 2; mostramos como o problema da existência de um ponto da curva com coordenadas no corpo K, i. e., da existência de uma solução em K de uma equação de 2^o grau em duas varíaveis, dependa da escolha do corpo base. Concluímos que uma cônica é isomorfa a $\mathbb{P}^1_K$ se, e só se, existe um ponto com coordenadas em K e portanto que nesse caso a correspondente equação de 2^o grau em duas varíaveis terá "aproximadamente" $\#(K)$ soluções "afins". Tratamos o caso $K = \mathbb{Q}$ e demonstramos o princípio local-global, ou de Hasse-Minkowski, para determinar a existência de uma (e portanto de infinitas) soluções com coordenadas racionais: existe uma solução em $\mathbb{Q}^2$ de uma equação de segundo grau em duas variáveis com coeficientes em $\mathbb{Z}$ dada por um polinômio irredutível sobre $\overline{\mathbb{Q}}$ se, e só se, existe uma solução em $\mathbb{R}^2$ e em $\mathbb{Q}_p^2$ para cada primo $p \geq 2$. Um resultado sutil, conhecido como Lemma de Hensel (o inventor dos números p-ádicos $\mathbb{Q}_p$), mostra que, essencialmente, a existência das soluções em $\mathbb{Q}_p^2$ pode-se reduzir ao estudo das soluções das equações "módulo p", i.e. ao estudo das soluções em $\mathbb{F}_p^2$ das correspondente equações "módulo p". Fechamos o capítulo mostrando que uma cônica definida sobre os corpos $K = \mathbb{F}_q$ e $K = k(C)$, corpo das funções de uma curva algébrica definida sobre um corpo algebricamente fechado k, admite sempre um ponto com coordenadas em K, i.e, as equações de segundo grau correspondentes têm sempre "quase" $\#(K)$ soluções "afins". Como consequência toda curva lisa de gênero 0 definida sobre essas classes de corpos á isomorfa a $\mathbb{P}^1_K$.

No terceiro capítulo definimos uma curva elíptica E sobre K como uma curva lisa de gênero 1 definida sobre K, que admita pelo menos un ponto $O \in E(K)$ com "coordenadas" em K. Mostramos que o estudo dessa classe de curvas é equivalente, se $\mathrm{char}(K) \neq 2, 3$, ao estudo das equações em duas variáveis de terceiro grau da forma $y^2 = x^3 + ax + b$ onde o polinômio $x^3 + ax + b \in K[x]$ não tem raízes múltiplas (o ponto O indo no único ponto "no infinito" da curva projetiva C correspondente). A partir disso mostraremos como os pontos com coordenadas em K de C, $C(K)$, possuem uma lei de grupo abeliano com $(0 : 1 : 0) \in C(K)$ seu elemento neutro. Observamos, como nesse caso um famoso exemplo de Selmer, a cúbica lisa definida

sobre $\mathbb{Q}$ pela equação $3x^3+4y^3+5=0$ não admite soluções racionais (nem ao infinito) mas admite soluções reais e em $\mathbb{Q}_p$ para cada primo $p \geq 2$. Assim o nosso estudo é o estudo de particulares classes de curvas de gênero 1 e esse exemplo mostra como o problema de determinar pontos em $E(K)$ possa ser muito sutil para qualquer corpo K. Quando não vazio permanece o problema de descrever a estrutura do grupo abeliano $E(K)$.

No quarto capítulo estudamos as isogenias entre curvas elípticas, i.e., os morfismos de curvas elípticas que são também homomorfismos de grupos. Aplicamos o estudo das isogenias para obter a cota de Hasse, conjecturada por E. Artin, $|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$ e mostramos com um exemplo, que esta cota é a melhor possível.

O quinto capítulo trata do importante teorema de Mordell que garante, para curvas elípticas E definidas sobre $\mathbb{Q}$, a finitude do número de geradores do grupo abeliano $E(\mathbb{Q})$ dos pontos "racionais". Isto, por sua vez, implica que $E(\mathbb{Q}) \simeq \mathbb{Z}^r \times E(\mathbb{Q})_{tors}$, onde $E(\mathbb{Q})_{tors}$ é o subgrupo finito dos pontos de torção. Esse resultado foi estendido mais tarde por Weil para o caso de corpos de números (extensões finitas de $\mathbb{Q}$) em dimensão maior, i.e., para variedades abelianas definidas sobre corpos de números. A demonstração apresentada é obtida com métodos "modernos": teoria das alturas e teorema de Mordell Fraco ("descida infinita") diferentes dos métodos originais de Mordell. Fechamos o capítulo com um exemplo que se $K = k(C)$ é o corpo das funções racionais de uma curva complexa C, então existem curvas elípticas E definidas sobre $k(C)$ tais que $E(k(C))$ não é finitamente gerado.

O sexto capítulo estuda em detalhes vários exemplos de curvas elípticas sobre $\mathbb{Q}$ e enuncia os teoremas de Mazur e de Nagell-Lutz que descrevem $E(\mathbb{Q})_{tors}$ e as únicas possibilidades que podem ocorrer.

Fechamos essa introdução dizendo que a demonstração de Faltings da conjectura de Mordell: se C é uma curva lisa de gênero $g \geq 2$ definida sobre um corpo de números K, então $\#C(K) < \infty$; e a demonstração de Wiles do teorema de Fermat (de fato um melhoramento do teorema de Faltings para as curvas lisas $x^n+y^n=1$ de gênero $g(n) = 1/2(n-1)(n-2) \geq 3$, se $n \geq 4$) completam o quadro da estrutura dos conjuntos $C(K)$ para corpos de números e se destacam, junto com a demonstração de Dwork, M. Artin, Grothendieck e Deligne das conjecturas de Weil, como os maiores sucessos da geometria aritmética do século passado.

Capítulo 1

Curvas Algébricas

Pretende-se neste capítulo fixar notação bem como enunciar alguns resultados de Geometria algébrica para curvas que adiante serão de fundamental importância para o nosso estudo. Embora as curvas elípticas sejam objetos de intenso estudo da teoria dos números, possuindo aplicações jamais imaginadas, seu ambiente natural é de fato a Geometria: afinal trata-se de uma "curva" e, como tal, as melhores ferramentas para tratar de curvas são geométricas. O que ocorre na realidade é a tentativa de fazer aritmética a partir da geometria e esta relação entre a aritmética e a geometria é a mais natural possível, pois, numa linearização grosseira, Teoria dos Números nada mais é do que procurar soluções inteiras ou racionais para polinômios, enquanto que a Geometria propõe-se a estudar a estrutura de uma curva ou variedade algébrica (zeros de um polinômio definido, de preferência, sobre um corpo algebricamente fechado). Ao agirmos desta forma estamos ampliando os horizontes, transcendendo, abstraindo e a abstração é um procedimento natural da matemática moderna e da vida: olhamos para o horizonte para enxergarmos melhor o que vai dentro de nós.

1.1 Notações

Este é um capítulo de referências que preferencialmente deve ser lido acompanhado por um bom livro de Geometria Algébrica. Na confecção deste trabalho o livro do [FULTON], o do [SHAFAREVICH] e os capítulos iniciais do [SILVERMAN] e [HINDRY-SILVERMAN] foram fundamentais. Recomenda-se uma leitura breve, sem se ater aos detalhes, pois como diz o título, nesta seção só fixamos notação para

o que há por vir.

Seja $k = \bar{k}$ um corpo algebricamente fechado. O conjunto

$$\mathbb{A}^n = \{P = (x_1, ..., x_n) \mid x_i \in \bar{k}\}$$

é *o espaço afim de dimensão n sobre k*.

O *espaço projetivo de dimensão n sobre k* é o quociente de $\mathbb{A}^{n+1}\backslash(0, ..., 0)$ pela seguinte relação de equivalência

$$P = (x_0, ..., x_n) \sim (y_0, ..., y_n) = Q$$

se existe $\lambda \in k^*$ tal que $P = \lambda Q$. Uma classe de equivalência $\{(\lambda x_0, ...\lambda x_n)\}$ será representada por $(x_0 : ... : x_n)$.

Se $K \subset k$, então

$$\mathbb{P}^n(K) = \{P \in \mathbb{P}^n \mid P^\sigma = P, \forall \sigma \in \mathrm{Gal}(\bar{K}/K)\}$$

é o *conjunto dos pontos K-racionais de* $\mathbb{P}^n$.

Seja $A \in \mathrm{Aut}[k^{n+1}]$ um k-automorfismo linear de k^{n+1}. Logo A induz um mapa bijetivo $\omega : \mathbb{P}^n \longrightarrow \mathbb{P}^n$ definido por:

$$[v] \longmapsto \omega([v]) = [A(v)]$$

De fato, para mostrarmos que ω está bem definido, basta notarmos que, como A é injetivo, teremos $A(v) \neq 0$ e, daí, $\omega([v]) = [A(v)] \in \mathbb{P}^n$ e notarmos também que $A(\lambda v) = \lambda A(v) \Longrightarrow \omega([v]) = [A(v)]$. Além do mais, se $[v]$ e $[w]$ são tais que $\omega([v]) = \omega([w])$, isto é, $[A(v)] = [A(w)]$ então teremos que existe $\lambda \in k^*$ tal que $A(w) = \lambda A(v)$. Como A é um automorfismo de k^{n+1}, teremos que $w = \lambda v$, isto é, $[w] = [v]$ e ω é injetiva. Seja $[v] \in \mathbb{P}^n$; por ser A um k-automorfismo de k^{n+1} existirá um $w \in k^{n+1}$ tal que $A(w) = v$, daí, $[v] = [A(w)] = A([w])$ o que nos mostra que ω é sobrejetivo. Mapas deste tipo são chamados de *projetividades* e formam um grupo indicado por $\mathbb{P}GL(n+1; k) = \dfrac{GL(n+1; k)}{\sim}$, onde $A \sim B$ se existir $\lambda \in K$ tal que $A = \lambda B$.

Para nós uma *curva algébrica sobre o corpo k* ou apenas *curva sobre k* será uma variedade projetiva sobre k de dimensão 1, usualmente denotada por C. Da definição de C, temos que

$$I(C) = \{f(X_0, ..., X_n) \in k[X_0, ..., X_n] \mid f : \text{homogêneo e } f(P) = 0, \forall P \in C\}$$

é um ideal primo e portanto $R = \dfrac{k[X_0, ..., X_n]}{I(C)}$ é um domínio. Seja D o corpo de frações de R.

Consideremos geradores de $I(C)$, $F_1, ..., F_r \in k[X_0, ..., X_n]$. Um ponto $P \in V$ é *não singular* se a matriz

$$\left(\frac{\partial F_i}{\partial X_j}(P)\right)_{\substack{1 \leq i \leq r \\ 0 \leq j \leq n}}$$

tem posto $n - 1$. Uma curva cujos pontos são todos não singulares é chamada de *não singular* ou *lisa*.

Seja $K \subset k$ um corpo. Diremos que uma curva C *está definida sobre* K se o ideal $I(C)$ for gerado por polinômios homogêneos em $K[X_0, ..., X_n]$. Neste caso escreveremos C/K ou $C_{|_K}$ para uma curva definida sobre K. Para uma curva $C_{|_K}$ definimos *o conjunto dos pontos K-racionais* de C como sendo

$$C(K) := \{P \in C \mid P^\sigma = P, \forall \sigma \in \mathrm{Gal}(\bar{K}/K)\}.$$

Uma curva $C_{|_K}$ é *lisa sobre* K quando dados $F_1, ..., F_r \in K[X_0, ..., X_n]$, geradores de $I(C)$, tivermos a matriz

$$\left(\frac{\partial F_i}{\partial X_j}(P)\right)_{\substack{1 \leq i \leq r \\ 0 \leq j \leq n}}$$

com posto igual a $n - 1$

A uma curva C associamos um corpo, dito *corpo de funções de* C e denotado por $k(C)$. Seus elemento são as funções racionais $F(X) = \dfrac{f(X)}{g(X)}$ que satisfazem:

1. f e g são polinômios homogêneos de mesmo grau;
2. $g \notin I(C)$;
3. duas funções f/g e f'/g' são identificadas se $fg' - f'g \in I(C)$.

Se $g(P) \neq 0$ então $F(P) = \dfrac{f(P)}{g(P)}$ é um valor bem definido para $F = \dfrac{f}{g} \in k(C)$. Neste caso dizemos que F *é regular em* P e o conjunto

$$k[C]_P = \{F \in K(C) \mid F \text{ é regular em } P\}$$

é chamado de *anel local de C em P*. Se C/K denotamos por $K(C)$ o corpo fixo de $\mathrm{Gal}(\bar{K}/K)$.

Sejam $C_1 \subseteq \mathbb{P}^m$ e $C_2 \subseteq \mathbb{P}^n$ duas curvas algébricas. Um *mapa racional de C_1 para C_2* é uma aplicação $\phi : C_1 \dashrightarrow C_2$ do tipo

$$\phi = [f_0 : f_1 : ... : f_n]$$

onde $f_i \in \bar{K}(C_1)$ e o ponto $[f_0(P) : f_1(P) : ... : f_n(P)] \in C_2$, para todo $P \in C_1$ tal que todos os f_i's são regulares em P. Se existir algum $\lambda \in \bar{K}^*$ tal que $\lambda f_i \in K(C_1), \forall i$ então diremos que ϕ *está definida sobre* K. Um mapa racional $\phi : C_1 \dashrightarrow C_2$ é *birracional* se ele possuir um mapa racional inverso $\psi : C_2 \dashrightarrow C_1$. Neste caso dizemos que C_1 e C_2 são *birracionalmente equivalentes* ou *birracionais*. Uma curva C é *racional* se C e $\mathbb{P}^1_k$ são birracionais.

Um mapa racional $\phi = [f_0 : ... : f_n] : C_1 \dashrightarrow C_2$ é *regular em $P \in C_1$* quando existe uma função $g \in \bar{K}(C_1)$ tal que $gf_0, gf_1, ..., gf_n$ são todos regulares em P e existe um i com $gf_i(P) \neq 0$. Um mapa racional de C_1 para C_2 que é regular em todos os pontos de C_1 é chamado de *morfismo*. Se existir um morfismo $\psi : C_2 \to C_1$ tal que $\psi \circ \phi$ e $\phi \circ \psi$ são os mapas identidades em C_1 e C_2, respectivamente, diremos que C_1 e C_2 são *isomorfas*. Se C_1, C_2 e ambos os mapas estão definidos sobre K, as curvas serão então *isomorfas sobre K*. Há portanto uma identificação entre os conjuntos $C_1(K)$ e $C_2(K)$ que preserva as propriedades "boas" de uma curva, bastando então o estudo de uma única curva numa classe de isomorfismo.

O primeiro resultado que merece destaque é o seguinte

Teorema 1.1.1 *Seja C uma curva e $P \in C$ um ponto não singular. Então $\bar{K}[C]_P$ é um domínio de valoração discreta.*
Prova: [FULTON], pg. 98. □

Ele é garantia de que para todo ponto $P \in C$, curva lisa, existe uma função $t \in \bar{K}(C)^*$ tal que para toda $f \in \bar{K}(C)$ não nula existe uma função $u_f \in \bar{K}(C)$ e um inteiro m tais que:
(i) t se anula em P;
(ii) $u_f(P) \neq 0$;
(iii) $f = u_f t^m$.

A função t é chamada de *parâmetro local para C no ponto P*. É fácil mostrar que o inteiro m não depende do parâmetro local escolhido e é um número bem definido

para toda $f \in \bar{K}(C)^*$. Chamamos a este número de *ordem de f no ponto P* que denotamos por $\text{ord}_P\ f$. Convenciona-se que $\text{ord}_P\ 0 = \infty$.

Se $P \in C$ é não singular diremos que $f \in \bar{K}(C)$ tem um *zero* em P, se $\text{ord}_P\ f > 0$; e que f tem *um pólo* quando $\text{ord}_P\ f < 0$. Se $\text{ord}_P\ f \geq 0$ diremos que f é *regular em P* e é possível calcular $f(P)$. Caso contrário f tem um pólo em P e escreve-se $f(P) = \infty$.

Teorema 1.1.2 *Seja C uma curva lisa e $f \in \bar{K}(C)$. Então existe uma quantidade finita de pontos em C nos quais f tem um zero ou um pólo. Ademais, se f não possui nenhum pólo então $f \in \bar{K}$.*
Prova: [HARTSHORNE], pg. 41. □

Teorema 1.1.3 *Seja C/K uma curva e $t \in K(C)$ um parâmetro local em algum ponto $P \in C$ liso. Então $K(C)/K(t)$ é uma extensão finita e separável.*
Prova: [SILVERMAN], pg. 22. □

1.2 Mapas racionais e morfismos

O primeiro resultado de importância nos fornece uma maneira "fácil" de obter morfismos sobre curvas lisas.

Teorema 1.2.1 *Sejam C uma curva, $V \subset \mathbb{P}^n$ uma variedade projetiva e $\phi : C \dashrightarrow V$ um mapa racional. Se $P \in C$ é um ponto não singular, então ϕ é regular em P. Em particular, todo mapa racional $\phi : C \dashrightarrow V$ é um morfismo, se C é uma curva lisa.*
Prova: [SILVERMAN], pg. 23. □

Teorema 1.2.2 *Sejam C_1 e C_2 duas curvas. Se $\phi, \psi : C_1 \to C_2$ são morfismos que coincidem num subconjunto denso de C_1 então $\phi = \psi$.*
Prova: [FULTON], pg. 146. □

Corolário 1.2.3 *Um morfismo birracional entre curvas lisas é um isomorfismo.*
Prova: Seja $\phi : C_1 \dashrightarrow C_2$ um morfismo birracional entre as curvas C_1 e C_2 e ψ sua inversa racional. Portanto $\phi \circ \psi$ se estende a um morfismo e coincide com a identidade num conjunto denso. Logo é a identidade. O mesmo argumento se aplica a $\psi \circ \phi$. □

Seja $C_{|_K}$ uma curva lisa. Toda função $f \in K(C)$ define um mapa racional de C em $\mathbb{P}^1$, que, pelo resultado anterior, é na realidade um morfismo definido sobre K:

$$f(P) = \begin{cases} (f(P) : 1) & \text{se } f \text{ é regular em } P \\ (1 : 0) & \text{se } f \text{ tem um pólo em } P \end{cases}$$

Por outro lado seja seja

$$\phi : C \to \mathbb{P}^1$$
$$\phi = [f : g]$$

um mapa racional definido sobre K. Caso $g = 0$, então $\phi = (1 : 0)$ será o mapa constante. Do contrário ϕ corresponde ao mapa definido pela função $\dfrac{f}{g} \in K(C)$. Se chamarmos de ∞ ao primeiro mapa, obtemos a seguinte correspondência biunívoca

$$K(C) \cup \{\infty\} \leftrightarrow \{\text{mapas } \phi : C \to \mathbb{P}^1 \text{ definidos sobre } K\}$$

Teorema 1.2.4 *Seja $\phi : C_1 \to C_2$ um morfismo entre curvas. Então ϕ é constante ou sobrejetivo.*
Prova: [HARTSHORNE], pg. 137. □

Sejam C_1/K e C_2/K curvas e $\phi : C_1 \to C_2$ um morfismo definido sobre K. A partir de ϕ podemos definir uma aplicação de $K(C_2)$ em $K(C_1)$ que será não constante se, e só se, ϕ for não constante (sobrejetiva, pelo teorema precedente). Denotado por ϕ^* este mapa é definido naturalmente por

$$\begin{array}{ccc} \phi^* : K(C_2) & \longrightarrow & K(C_1) \\ f & \longmapsto & \phi^*(f) = f \circ \phi \end{array}$$

e caso ϕ seja não constante ϕ^* determina um homomorfismo injetor de corpos que fixa K, isto é, $\phi^*(K) = K$.

Teorema 1.2.5 *Sejam C_1/K e C_2/K curvas.*
(a) Seja $\phi : C_1 \to C_2$ um mapa não constante definido sobre K. Então $K(C_1)/\phi^*(K(C_2))$ é uma extensão finita.
(b) Seja $\iota : K(C_2) \to K(C_1)$ uma injeção de corpos que fixa os elementos de K. Nestas condições existe um único mapa não constante $\phi : C_1 \to C_2$ entre curvas lisas, definido sobre K, tal que $\phi^* = \iota$.
(c) Seja $K(C_1)/L$ uma extensão finita contendo K. Então existe uma curva lisa C'/K, única a menos de isomorfismo, e um mapa não constante $\phi : C \to C'$ definido sobre K tal que $\phi^*(K(C')) = L$.
Prova: (a) [HARTSHORNE], pg. 137;
(b) [SILVERMAN], pg. 25;
(c)[HARTSHORNE], pg. 45. □

Seja $\phi : C_1 \to C_2$ um mapa. Caso ϕ seja sobrejetivo, ao número $[K(C_1) : \phi^*(K(C_2))]$ chamamos de *grau de ϕ* e denotamos por $\deg \phi$. Por convenção, o grau do mapa constante é zero. Se a extensão $K(C_1)/\phi^*(K(C_2))$ é separável, inseparável ou puramente inseparável, diremos que o mapa ϕ é *separável, inseparável ou puramente inseparável*, respectivamente, e denotamos o grau de separabilidade e inseparabilidade da extensão por $\deg_s \phi$ e $\deg_i \phi$, respectivamente.

Corolário 1.2.6 *Sejam C_1 e C_2 curvas lisas e seja $\phi : C_1 \to C_2$ com $\deg \phi = 1$. Então ϕ é um isomorfismo.*
Prova: [SILVERMAN], pg. 25. □

Para um mapa não constante definido sobre K, $\phi : C_1 \to C_2$, entre curvas, definimos

$$\begin{aligned} \phi_* &: K(C_1) \to K(C_2) \\ \phi_* &= (\phi)^{-1} \circ \mathrm{Norm}_{K(C_1)/\phi^*(K(C_2))} \end{aligned}$$

onde o resultado (**1.2.5**, pg. 14) assegura a existência da função norma.

Sejam C_1 e C_2 curvas não singulares e $\phi : C_1 \to C_2$ um mapa não constante entre elas. Seja $t_{\phi(P)} \in K(C_2)$ um parâmetro local para C_2 em $\phi(P)$. O número

$$\mathrm{ord}_P\left(\phi^*(t_{\phi(P)})\right) \geq 1$$

independe da escolha do parâmetro local e é portanto uma função de P e ϕ chamada de *índice de ramificação de ϕ em P* e denotada por $e_\phi(P)$. Diremos que *ϕ é não ramificado em P* se $e_\phi(P) = 1$. ϕ é dito *não ramificado* se ele for não ramificado em todo ponto $P \in C_1$.

Teorema 1.2.7 *Seja $\phi : C_1 \to C_2$ um mapa não constante entre curvas lisas.*
(a) Para todo $Q \in C_2$ vale

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi$$

(b) Para todos os pontos $Q \in C_2$, a menos de um conjunto finito, vale

$$\#\phi^{-1}(Q) = \deg_s \phi$$

(c) Seja $\psi : C_2 \to C_3$ um outro mapa não constante. Então para todo $P \in C_1$

$$e_{\psi\circ\phi}(P) = e_\phi(P) \cdot e_\psi(\phi(P))$$

(d) $\operatorname{ord}_{P_1} \ f \circ \phi = e_\phi(P_1) \cdot \operatorname{ord}_{\phi(P_1)} \ f, \qquad \forall f \in K(C_2)^*.$
Prova: (a)[HARTSHORNE], pg. 138;
(b) [HARTSHORNE], pg. 137;
(c) [SILVERMAN], pg. 28;
(d) [SILVERMAN], pg. 28. □

Corolário 1.2.8 *Um mapa $\phi : C_1 \to C_2$ é não ramificado se, e somente se, $\#\phi^{-1}(Q) = \deg \phi$, para todo $Q \in C_2$.*
Prova: Do item (a) temos que $\#\phi^{-1}(Q) = \deg \phi$ é equivalente a

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \#\phi^{-1}(Q)$$

Como $e_\phi(P) \geq 1$ isto só pode ocorrer se, e somente se, $e_\phi(P) = 1$ □

1.3 Divisores

Um *divisor* de uma curva C é uma soma formal do tipo

$$D = \sum_{P \in C} n_P(P)$$

com $n_P \in \mathbb{Z}$ e $n_P = 0$ para todos menos um número finito de $P \in C$. Seja $\mathrm{Div}(C)$ o conjunto de todos os divisores de C. Ao definirmos a soma de dois divisores da maneira mais natural possível, dotamos $\mathrm{Div}(C)$ de uma estrutura de grupo e passamos a chamá-lo de *o grupo de divisores de* C. O *grau* de um divisor é o número

$$\deg D = \sum_{P \in C} n_P$$

O subgrupo de $\mathrm{Div}(C)$

$$\mathrm{Div}^0(C) = \{D \in \mathrm{Div}(C) \mid \deg D = 0\}$$

é chamado de *subgrupo dos divisores de grau 0.*

Um divisor $D = \sum_{P \in C} n_P(P)$ é dito *efetivo* ou *positivo* quando $n_P \geq 0, \forall P \in C$, e a esta característica representamos por $D \geq 0$. Para dois divisores $D_1, D_2 \in \mathrm{Div}(C)$ escreveremos

$$D_1 \geq D_2$$

para indicar que o divisor $D_1 - D_2$ é efetivo.

Se C está definida sobre K, podemos definir uma ação do grupo $\mathrm{Gal}(\bar{K}/K)$ sobre $\mathrm{Div}(C)$ (e $\mathrm{Div}^0(C)$) da seguinte maneira: para um $\sigma \in \mathrm{Gal}(\bar{K}/K)$

$$D^\sigma = \sum_{P \in C} n_P(P^\sigma)$$

Diremos então que D *está definido sobre* K se $D^\sigma = D, \forall \sigma \in \mathrm{Gal}(\bar{K}/K)$ e ao conjunto destes divisores, o *grupo de divisores definido sobre* K, denotaremos por $\mathrm{Div}_K(C)$ ($\mathrm{Div}^0_K(C)$, respectivamente).

Se C for uma curva lisa, por (**1.1.2**, pg. 12), podemos para cada $f \in \bar{K}(C)^*$ definir o divisor

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P\ (f)(P)$$

É fácil verificar que para $\sigma \in \mathrm{Gal}(\bar{K}/K)$ vale

$$\mathrm{div}(f^\sigma) = \mathrm{div}(f)^\sigma$$

e portanto $f \in K(C)$ implica que $\mathrm{div}(f) \in \mathrm{Div}_K(C)$. Segue prontamente das definições e do fato de ser ord_P uma valoração em $\bar{K}(C)$ que o mapa

$$\mathrm{div} : \bar{K}(C) \to \mathrm{Div}(C)$$

é um homomorfismo de grupos abelianos.

Diremos que um divisor D é *principal* se existir $f \in \bar{K}(C)^*$ tal que $D = \mathrm{div}(f)$. Os divisores principais formam um subgrupo de $\mathrm{Div}(C)$ e o quociente $\mathrm{Pic}(C)$ de $\mathrm{Div}(C)$ por este subrupo é chamado de *o grupo da classe de divisores* ou *grupo de Picard*. Dois divisores D e D' são *linearmente equivalentes*, denotado por $D \sim D'$, quando eles determinam a mesma classe em $\mathrm{Pic}(C)$ ou, equivalentemente, quando o divisor $D - D'$ é principal. Ao subgrupo de $\mathrm{Pic}(C)$ fixado por $\mathrm{Gal}(\bar{K}/K)$ denotaremos por $\mathrm{Pic}_K(C)$.

Teorema 1.3.1 *Seja C uma curva não singular e $f \in \bar{K}(C)^*$. Então:*
(a) $\mathrm{div}(f) = 0$ *se, e somente se,* $f \in \bar{K}^*$,
(b) $\deg(\mathrm{div}(f)) = 0$.
Prova: (a) [SILVERMAN], pg. 32;
(b) [FULTON], pg. 188. □

O item (b) do teorema acima nos diz que o subgrupo dos divisores principais está contido em $\mathrm{Div}^0(C)$, e portanto faz sentido tomarmos o quociente de $\mathrm{Div}^0(C)$ pelo subgrupo dos divisores principais. Chamamos a este grupo quociente de *o subgrupo da parte de grau 0 da classe de divisores* e denotamos por $\mathrm{Pic}^0(C)$. $\mathrm{Pic}^0_K(C)$ é a parte de $\mathrm{Pic}^0(C)$ deixada fixa pela ação de $\mathrm{Gal}(\bar{K}/K)$.

Um mapa não constante $\phi : C_1 \to C_2$ entre duas curvas lisas induz dois homomorfismos entre os respectivos grupos de divisores das curvas: um no mesmo sentido de ϕ e outro no sentido contrário, definidos pela extensão $\mathbb{Z}$ linear das seguintes associações

$$\begin{array}{ccc} \phi^* : \mathrm{Div}(C_2) & \longrightarrow & \mathrm{Div}(C_1) \\ Q & \longmapsto & \displaystyle\sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P) \end{array} \qquad \text{e} \qquad \begin{array}{ccc} \phi_* : \mathrm{Div}(C_1) & \longrightarrow & \mathrm{Div}(C_2) \\ P & \longmapsto & (\phi(P)) \end{array}$$

Estes mapas satisfazem

Teorema 1.3.2 *Seja $\phi : C_1 \to C_2$ um mapa não constante entre curvas lisas. Então*
(a) $\deg(\phi^*(D)) = \deg\phi \cdot \deg D$, *para todo* $D \in \mathrm{Div}(C_2)$
(b) $\phi^*(\mathrm{div}\, f) = \mathrm{div}(\phi^*(f))$, *para todo* $f \in \bar{K}(C_2)^*$
(c) $\deg(\phi_*(D)) = \deg D$, *para todo* $D \in \mathrm{Div}(C_1)$
(d) $\phi_*(\mathrm{div}\, f) = \mathrm{div}(\phi_*(f))$, *para todo* $f \in \bar{K}(C_1)^*$
(e) $\phi_* \circ \phi^*$ *age como a multiplicação por* $\deg\phi$ *em* $\mathrm{Div}(C_2)$
(f) Se $\psi : C_2 \to C_3$ *é um outro mapa não constante e* C_3 *é lisa então*

$$(\psi \circ \phi)^* = \phi^* \circ \psi^* \qquad e \qquad (\psi \circ \phi)_* = \psi_* \circ \phi_*$$

Prova: [SILVERMAN], pg 34. □

Portanto ϕ^* e ϕ_* restringe-se a homomorfismos entre $\mathrm{Div}^0(C_1)$ e $\mathrm{Div}^0(C_2)$ e induzirá também os homomorfismos

$$\phi^* : \mathrm{Pic}^0(C_2) \to \mathrm{Pic}^0(C_1) \qquad \text{e} \qquad \phi_* : \mathrm{Pic}^0(C_1) \to \mathrm{Pic}^0(C_2)$$

1.4 Diferenciais

Para uma curva C definimos o *espaço das formas diferenciais*, Ω_C, como sendo o $\bar{K}(C)$-espaço vetorial gerado pelos símbolos da forma dx, para todo $x \in \bar{K}(C)$, submetidos às regras de "diferenciação "
(i) $d(x+y) = dx + dy$, para todo $x, y \in \bar{K}(C)$
(ii) $d(xy) = xdy + ydx$, para todo $x, y \in \bar{K}(C)$
(iii) $dc = 0$, para todo $c \in \bar{K}$.

Teorema 1.4.1 *Para uma curva C temos*
(a) Ω_C *é um* $\bar{K}(C)$*-espaço vetorial unidimensional*
(b) Se $x \in \bar{K}(C)$ *então* dx *é uma* $\bar{K}(C)$ *base para* Ω_C *se, e somente se,* $\bar{K}(C)/\bar{K}(x)$ *é uma extensão finita e separável.*
Prova: (a) e (b) [MATSUMURA], pg. 210. □

Ainda uma vez mais, um mapa não constante $\phi : C_1 \to C_1$ entre curvas induz um mapa entre os espaços Ω_{C_1} e Ω_{C_2}. Este mapa é obtido a partir do mapa

$\phi^* : \bar{K}(C_2) \to \bar{K}(C_1)$ da seguinte maneira:

$$\begin{array}{ccc} \phi^* : \Omega_{C_2} & \longrightarrow & \Omega_{C_1} \\ fdx & \longmapsto & \phi^*(fdx) = \phi^*(f)d(\phi^*(x)) \end{array}$$

onde dx é uma $\bar{K}(C_2)$ base para Ω_{C_2}. Não é difícil mostrar que ϕ^*, assim definido, não depende da base escolhida. Desta aplicação obtemos um critério bastante útil para determinar quando ϕ é ou não separável.

Teorema 1.4.2 *Seja $\phi : C_1 \to C_2$ um mapa não constante entre curvas. Então ϕ é separável se, e só se, a aplicação*

$$\phi^* : \Omega_{C_2} \to \Omega_{C_1}$$

é não nula.
Prova: [SILVERMAN], pg. 35. □

Teorema 1.4.3 *Seja $P \in C$ e $t \in \bar{K}(C)^*$ um parâmetro local em P.*
(a) Para todo $\omega \in \Omega_C$ existe uma única função $g \in \bar{K}(C)$, dependendo de ω e t, tal que

$$\omega = gdt$$

Denotamos g por ω/dt.
(b) Seja $f \in \bar{K}(C)$ uma função regular em P. Então df/dt também é regular em P.
(c) O número

$$\mathrm{ord}_P\,(\omega/dt)$$

não depende da escolha do parâmetro local t mas apenas de ω e P. Chamamos a esta quantia da ordem de ω em P e a denotamos por $\mathrm{ord}_P\,(\omega)$.
(d) Seja $x \in \bar{K}(C)$ tal que $\bar{K}(C)/\bar{K}(x)$ é separável e $x(P) = 0$. Então para todo $f \in \bar{K}(C)$

$$\mathrm{ord}_P\,(fdx) = \mathrm{ord}_P\,(f) + \mathrm{ord}_P\,(x) - 1$$

(e) Para todos os pontos a menos de um número finito $P \in C$ temos

$$\mathrm{ord}_P\,(\omega) = 0$$

Prova: [SILVERMAN], pg 36. □

Desta forma podemos associar a um diferencial $\omega \in \Omega_C$ o divisor

$$\mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P\ (\omega)(P)$$

Um diferencial $\omega \in \Omega_C$ é *holomorfo* (*ou regular*) quando $\mathrm{div}(\omega)$ é efetivo. Se $\mathrm{div}(\omega) \leq 0$ diremos que ω *não se anula*.

Se $\omega_1, \omega_2 \in \Omega_C^*$ então (**1.4.1**, pg. 18) implica que existe uma função $f \in \bar{K}(C)^*$ tal que $\omega_1 = f\omega_2$ e portanto

$$\mathrm{div}(\omega_1) = \mathrm{div}(f) + \mathrm{div}(\omega_2)$$

ou seja, os divisores de diferenciais não nulos são todos linearmente equivalentes. A classe em $\mathrm{Pic}(C)$ determinada pelo divisor de uma diferencial não nula é chamada de *classe canônica* e qualquer divisor nesta classe é dito um *divisor canônico*.

1.5 O teorema de Riemann-Roch

Observemos que para uma função $f \in \bar{K}(C)$ uma desigualdade do tipo

$$\mathrm{div}(f) \geq (Q) - 2(P)$$

torna conciso o fato de que f tem um zero em Q e um pólo de ordem no máximo 2 em P. Esta é uma das razões pelas quais se estuda divisores de uma curva: pode nos trazer informações relevantes sobre as funções desta curva. É ela que também motiva a definição do seguinte $\bar{K}$-espaço vetorial

$$\mathcal{L}(D) = \{f \in \bar{K}(C)^* \mid \mathrm{div}\, f \geq -D\} \cup 0.$$

Teorema 1.5.1 *Seja* $D \in \mathrm{Div}(C)$.
(a) Se $\deg D < 0$ *então*

$$\mathcal{L}(D) = 0$$

(b) $\mathcal{L}(D)$ *é um* $\bar{K}$*-espaço vetorial de dimensão finita.*
(c) Se $D' \in \mathrm{Div}(C)$ *é tal que* $D' \sim D$ *então*

$$\mathcal{L}(D) = \mathcal{L}(D').$$

Prova: [FULTON], pg. 192. □

Sendo assim escreveremos

$$\ell(D) = \dim_{\bar{K}} \mathcal{L}(D)$$

Podemos associar a um divisor $D \in \mathrm{Div}(C)$ tal que $\ell(D) = n + 1$ um mapa racional $\phi_D : C \dashrightarrow \mathbb{P}^n$ definido por

$$\phi_D(P) \longmapsto (f_0 : ... : f_n)$$

onde $\{f_0, ..., f_n\}$ é uma base para $\mathcal{L}(D)$. Note que este mapa depende da escolha da base. Ele satisfaz a seguinte propriedade

Teorema 1.5.2 *ϕ_D é um morfismo tal que C é isomorfo a $\phi_D(C)$ se, e somente se, para todos os pontos $P, Q \in C$ tivermos*

$$\ell(D - P - Q) = \ell(D) - 2$$

Prova: [HARTSHORNE], pg. 307. □

Um mapa $\phi : C \to \mathbb{P}^r$ tal que $\phi(C) \simeq C$ é chamado de um *um mergulho de C em $\mathbb{P}^r$*. Neste caso o teorema nos dá um critério para decidir quando o mapa associado ϕ_D é um mergulho de C em $\mathbb{P}^n$.

E finalmente temos o celebrado

Teorema 1.5.3 (Riemann-Roch) *Seja C uma curva lisa e K_C um divisor canônico em C. Existe um inteiro $g \geq 0$, tal que $\forall D \in \mathrm{Div}(C)$ temos*

$$\ell(D) - \ell(K_C - D) = \deg D - g + 1$$

Prova: [FULTON], pg. 210. □

Chamamos a este número g de *gênero da curva* pois, como é mostrado abaixo, ele depende apenas de C e é ainda um invariante da classe de isomorfismo da curva

Corolário 1.5.4 *(a)* $\ell(K_C) = g$.
(b) $\deg K_C = 2g - 2$.
(c) Se $\deg D > 2g - 2$, *então*

$$\ell(D) = \deg D - g + 1.$$

Prova: (a) Tomemos $D = 0$. Então $\mathcal{L} = \bar{K}$ já que uma função sem pólos também não pode possuir zeros (**1.1.2**, pg. 12). Portanto $\ell(0) = 1$ e

$$1 - \ell(K_C) = 0 - g + 1.$$

(b) Tomando $D = K_C$ no Riemann-Roch encontramos

$$\begin{aligned} \ell(K_C) - \ell(0) &= \deg(K_C) - g + 1 \\ g - 1 = \deg(K_C) - g + 1 & \end{aligned}$$

(c) Do item anterior temos que

$$\deg(K_C - D) < 0$$

e portanto

$$\ell(K_C - D) = 0$$

□

Corolário 1.5.5 *Duas curvas isomorfas possuem o mesmo gênero.*
Prova: Seja $\phi : C_1 \to C_2$ um isomorfismo entre as curvas C_1 e C_2 de gênero g_1 e g_2 respectivamente. Logo ϕ é não ramificado e tem grau 1. Além disso, se K_{C_1} é um divisor canônico de C_1 então $\phi^*(K_{C_1}) = K_{C_2}$ é um divisor canônico de C_2. Daí, pelo corolário anterior, temos

$$\begin{aligned} 2g_2 - 2 &= \deg(K_{C_2}) = \deg(\phi^*(K_{C_2})) = \deg\phi \deg(K_{C_2}) = 2g_1 - 2 \\ g_2 &= g_1 \end{aligned}$$

□

Teorema 1.5.6 (Hurwitz) *Considere uma aplicação não constante e separável* $\phi : C_1 \to C_2$ *entre curvas não singulares de gênero* g_1 *e* g_2 *respectivamente. Portanto*

$$2g_1 - 2 \geq (\deg\phi)(2g_2 - 2) + \sum_{P \in C} (e_\phi(P) - 1)$$

A igualdade vale se, e somente se, ocorre
(i) $\mathrm{char}(K) = 0$*; ou*
(ii) $\mathrm{char}(K) = p > 0$ *e* p *não divide* $e_\phi(P)$*, para todo* $P \in C_1$.
Prova: [SILVERMAN], pg 41. □

Corolário 1.5.7 (Fórmula do grau-gênero) *Seja* $F(X, Y, Z) \in K[X, Y, Z]$ *um polinômio homogêneo de grau* $d \geq 1$ *e suponha que a curva* C *em* $\mathbb{P}^2$ *dada pela equação* $F = 0$ *seja lisa. Então*

$$g(C) = \frac{(d-1)(d-2)}{2}.$$

Prova: Podemos supor $K = \bar{K}$ e, por simplicidade, vamos supor que K seja um corpo de característica zero.

Aplicando uma projetividade, se necessário, podemos supor que $(0 : 1 : 0) \notin C$, que a reta $z = 0$ não seja tangente a C. Logo o mônomio Y^d deve figurar no polinômio F, cuja representação afim será

$$F(X, Y) = Y^d + a_1(X)Y^{d-1} + ... + a_d(X)$$

com os $a_i(X) \in K[X]$. Desta forma a projeção de C do ponto $(0 : 1 : 0)$ sobre a reta de equação $Y = 0$

$$\begin{array}{ccc} \phi : C & \longrightarrow & \mathbb{P}^1 \\ (x : y : z) & \longmapsto & (x : z) \end{array}$$

é um morfismo de grau d (a resultante de F e $\partial F/\partial Y$, como polinômios em $K[X][Y]$, não é identicamente nula porque F é irredutível; assim por uma escolha de $\widetilde{x} \in K$ qualquer, temos que $F(\widetilde{x}, Y)$ tem d raízes distintas e a conclusão segue da fórmula do grau; ou de outra forma, temos que $\phi^*(K(\mathbb{P}^1)) = K(x, z)$ e portanto $\deg \phi = [K(x, y, z) : K(x, z)] = d$ já que y satisfaz um polinômio irredutível de grau d a coeficientes em $K(x, z)$). Seja $l_{\widetilde{x}}$ a reta de equação afim $x = \widetilde{x}$ e seja C' a curva de equação $\dfrac{\partial F}{\partial Y}$. Por hipótese C e C' se cortam ao finito e em um número finito de pontos. Se $P = (\widetilde{x} : \widetilde{y} : 1) \in C \cap C'$, podemos escolher $y - \widetilde{y}$ como parâmetro local de C em P, $\dfrac{\partial F}{\partial X}(P) \neq 0$. Desta forma temos que a função $x - \widetilde{x}$ é um parâmetro local no ponto $(\widetilde{x} : 1)$ e portanto, pela definição de $e_\phi(P)$,

$$\phi^*(x - \widetilde{x}) = F(\widetilde{x}, y) = (y - \widetilde{y})^{e_\phi(P)}\phi(y)$$

com $\phi(\widetilde{y}) \neq 0$. E pela definição de multiplicidade de interseção segue que

$$\text{mult}_P(l_{\widetilde{x}} \cap C) = e_\phi(P).$$

Vemos que um ponto P, necessariamente ao finito, será de ramificação se sua tangente passar por $(0:1:0)$, e portanto os possíveis pontos de ramificação estarão contidos nos pontos de interseção das curvas C e C'. Vamos calcular a multiplicidade de interseção de C e C'. Seja $P = (\widetilde{x} : \widetilde{y} : 1) \in C$. De

$$\frac{\partial F}{\partial Y}(\widetilde{x}, Y) = e_\phi(P)(Y - \widetilde{y})^{e_\phi(P)-1}\phi(Y) + (Y - \widetilde{y})^{e_\phi(P)}\frac{\partial \phi}{\partial Y} = (Y - \widetilde{y})^{e_\phi(P)-1}\psi(Y)$$

com $\psi(\widetilde{y}) \neq 0$ e, pela definição, temos $\text{mult}_P(C \cap C') = e_\phi(P) - 1$ para cada $P \in C \cap C'$ e logo para cada $P \in C$.

Pelo teorema de Bézout temos

$$d(d-1) = \sum_{P \in C} \text{mult}_P(C \cap C') = \sum_{P \in C}(e_\phi(P) - 1).$$

Uma aplicação do teorema de Hurwitz para o mapa ϕ fornece

$$\begin{aligned} 2g - 2 &= d(-2) + \sum_{P \in C}(e_\phi(P) - 1) \\ 2g - 2 &= -2d + d(d-1) \\ g &= \frac{(d-1)(d-2)}{2} \end{aligned}$$

E o resultado segue.

Pela observação que fizemos acima sobre o índice de ramificação, vemos que dizer que $e_\phi(P) > 2$ é o mesmo que afirmar que a reta que passa por P e $(0:1:0)$ é uma tangente inflexional. Como os pontos de inflexão são em número finito, podemos sempre encontrar uma projetividade tal que $(0:1:0) \notin C$ e as retas tangentes dos pontos de inflexão não passam por $(0:1:0)$ e portanto podemos até afirmar que a menos de uma projetividade temos exatamente $d(d-1)$ pontos de ramificação . □

O próximo resultado nos diz que se C e D estão definidos sobre K então $\mathcal{L}(D)$ também está

Teorema 1.5.8 *Seja C/K uma curva lisa e seja $D \in \mathrm{Div}_K(C)$. Então $\mathcal{L}(D)$ tem uma base consistindo de funções em $K(C)$.*
Prova: [SILVERMAN], pg 40. □

Capítulo 2

Curvas de Gênero 0

2.1 Cônicas

Por *cônica projetiva* $\mathcal{C}$ *sobre o corpo* K, denotada por $\mathcal{C}/K$ ou $\mathcal{C}_{|_K}$, entendemos o conjunto algébrico definido por um polinômio homôgeneo de grau dois $F(X_0, X_1, X_2) \in K[X_0, X_1, X_2]$ sem fatores irredutíveis repetidos. Portanto

$$\mathcal{C}(K) = \{p \in \mathbb{P}^2(K) \mid F(p) = 0\}.$$

A cônica se diz *irredutível* se $F(\mathbf{X})$ é irredutível em $\overline{K}[X_0, X_1, X_2]$. Note que toda cônica irredutível é também uma curva.

Se $\omega : \mathbb{P}^2 \to \mathbb{P}^2$ é uma projetividade dada por um automorfismo A de K^3 podemos obter a partir da cônica $\mathcal{C}$ uma outra cônica que é justamente a imagem $\omega(\mathcal{C})$ de $\mathcal{C}$ por ω. $\omega(\mathcal{C})$ será dada pelo polinômio

$$\begin{aligned} \tilde{F}(X_0, X_1, X_2) &= (F \circ A^{-1})(X_0, X_1, X_2) \\ &= F(\sum_{j=0}^{2} b_{0j}X_j, \sum_{j=0}^{2} b_{1j}X_j, \sum_{j=0}^{2} b_{2j}X_j) \end{aligned}$$

onde $A^{-1} = (b_{ij})_{0 \leq i,j \leq 2}$ é a inversa de A.

Duas cônicas C e $\tilde{C}$ são *projetivamente equivalentes* se existir uma projetividade $\omega : \mathbb{P}^2 \to \mathbb{P}^2$ tal que $\omega(C) = \tilde{C}$. Se a cônica for irredutível então uma projetividade ω induz um isomorfismo sobre K entre as cônicas irredutíveis $\mathcal{C}$ e $\omega(\mathcal{C})$.

Seja K um corpo de característica $\neq 2$.

Consideremos a cônica $\mathcal{C}_{|_K}$ definida por um polinômio $F(X_0, X_1, X_2) \in K[X_0, X_1, X_2]$ do tipo

$$\begin{aligned} F(X_0, X_1, X_2) &= \sum_{0 \leq i,j \leq 2} f_{ij} X_i X_j \\ &= f_{00}X_0^2 + f_{11}X_1^2 + f_{22}X_2^2 + f_{01}X_0X_1 + f_{02}X_0X_2 + f_{12}X_1X_2. \end{aligned}$$

Pondo:

$$M := \begin{pmatrix} f_{00} & f_{10}/2 & f_{20}/2 \\ f_{10}/2 & f_{11} & f_{21}/2 \\ f_{20}/2 & f_{21}/2 & f_{22} \end{pmatrix}$$

poderemos, então, escrever F da seguinte forma:

$$F(X_0, X_1, X_2) = \begin{pmatrix} X_0 & X_1 & X_2 \end{pmatrix} M \begin{pmatrix} X_0 \\ X_1 \\ X_2 \end{pmatrix}.$$

Neste caso diremos que a matriz M *representa a cônica* $\mathcal{C}$ ou, equivalentemente, que $\mathcal{C}$ *é representada por* M.

Definimos o *posto* de uma cônica como sendo o posto da matriz que a representa. Observemos que, por um fato elementar de Álgebra Linear, duas cônicas projetivamente equivalentes tem mesmo posto.

Temos o seguinte resultado.

Teorema 2.1.1 *Uma matriz simétrica $M \in \mathcal{M}(3; K)$ representa uma cônica definida sobre K se, e só se, posto$(M) \geq 2$. A cônica correspondente é redutível se, e só se, posto$(M) = 2$. Portanto posto$(M) = 3$ se, e só se, a cônica é irredutível; e posto$(M) = 2$ se, e só se, o polinômio que define a cônica é um produto de dois fatores distintos de grau 1 em $\overline{K}[X_0, X_1, X_2]$, i.e., não proporcionais por uma costante não nula.*

Prova: Por ser a matriz M simétrica, podemos encontrar $A = (a_{ij})_{0 \leq i,j \leq 2}$ invertível de forma que:

$$(A^{-1})^t M A^{-1} = \begin{pmatrix} b_0 & 0 & 0 \\ 0 & b_1 & 0 \\ 0 & 0 & b_2 \end{pmatrix}.$$

Em outras palavras: encontra-se uma projetividade $\omega : \mathbb{P}^2 \to \mathbb{P}^2$ de forma tal que a cônica $\mathcal{C}$ é isomorfa à cônica $\tilde{\mathcal{C}} = \omega(\mathcal{C})$ dada pelo polinômio $\tilde{F}(X_0, X_1, X_2) = b_0X_0^2 + b_1X_1^2 + b_2X_2^2$.

Portanto M representará uma cônica se, e somente se, $b_0b_1 \neq 0$ (sem perda alguma de generalidade); e isto ocorre se, e somente se, posto$(M) \geq 2$.

Para a parte final, suponhamos que F seja redutível. Então teremos $F = L_1 \cdot L_2$, com $L_1 = l_0X_0 + l_1X_1 + l_2X_2$ e $L_2 = m_0X_0 + m_1X_1 + m_2X_2$, $L_i \in \bar{K}[X_0, X_1, X_2]$ e $l_0 \cdot m_0 \neq 0$. Não podemos ter $L_1 = \alpha L_2$, $\alpha \in K^*$, pois F define uma cônica. Então $[L_1] \neq [L_2]$, donde concluímos que $l_0m_1 \neq l_1m_0$. Portanto se fizermos $X_0 \to L_1$, $X_1 \to L_2$ e $X_2 \to X_2$ teremos uma projetividade ω tal que $\omega(\mathcal{C}) = X_0X_1$, cujo posto é 2.

Por outro lado, pelo que vimos, podemos encontrar uma projetividade ω de forma que $\mathcal{C}$ é isomorfa a cônica $\tilde{\mathcal{C}} = \omega(\mathcal{C})$ definida por $\tilde{F}(X_0, X_1, X_2) = b_0X_0^2 + b_1X_1^2 + b_2X_2^2$. Se posto$(M) = 2$, então teremos que $\mathcal{C}$ é projetivamente equivalente a $b_0X_0^2 + b_1X_1^2 = (\sqrt{b_0}X_0^2 + \sqrt{-b_1}X_1^2)(\sqrt{b_0}X_0^2 - \sqrt{-b_1}X_1^2)$. Ou seja, $\mathcal{C}$ é redutível sobre $\bar{k}$. □

Notemos que a cônica $\mathcal{C}$ será singular em $P \in \mathbb{P}^2_{\bar{K}}$ se, e somente se, for singular em $\omega(P) = (x_0 : x_1 : x_2) \in \mathbb{P}^2_{\bar{K}}$ e isto ocorrerá caso:

$$\frac{\partial \tilde{F}}{\partial X_i}(P) = 2b_ix_i = 0$$

Como pelo menos um dos x_i's é não nulo, a cônica será singular se, e somente se, um dos b_i's for nulo. Equivalentemente, $\mathcal{C}$ é lisa se, e só se, $\det M \neq 0$. Obtendo o seguinte resultado:

Corolário 2.1.2 *Seja $\mathcal{C}$ uma cônica representada por uma matriz M. As seguintes afirmações são equivalentes:*
(i) $\mathcal{C}$ é lisa;
(ii) posto$(M) = 3$*;*
(ii) $\mathcal{C}$ é irredutível. □

Além disso, as cônicas irredutíveis gozam da seguinte propriedade

Teorema 2.1.3 *Seja $\mathcal{C}_{|_K}$ uma cônica lisa tal que $\mathcal{C}(K) \neq \emptyset$. Então $\mathcal{C}_{|_K}$ é projetiva-*

mente equivalente sobre K a cônica de equação $X^2 - YZ$.
Prova: A menos de uma projetividade podemos supor que $(0:1:0) \in \mathcal{C}$ e que $Z = 0$ é a reta tangente no ponto $(0:1:0)$. Suponhamos que $\mathcal{C}$ seja dada pelo polinômio

$$F(X,Y,Z) = a_0X^2 + a_1Y^2 + a_2Z^2 + a_3XY + a_4XZ + a_5YZ = 0$$

Logo

$$\begin{aligned} 0 = F(0:1:0) &= a_1 \\ 0 = \frac{\partial F}{\partial X}(0:1:0) &= a_3 \\ 0 = \frac{\partial F}{\partial Y}(0:1:0) &= a_1 \\ 0 \neq \frac{\partial F}{\partial Z}(0:1:0) &= a_5 \end{aligned}$$

ou seja, $F(X,Y,Z) = aX^2 + bZ^2 + cXZ + dYZ$ e a matriz que representa $\mathcal{C}$ é

$$M = \begin{pmatrix} a & 0 & c/2 \\ 0 & 0 & d/2 \\ c/2 & d/2 & b \end{pmatrix}$$

Como, estamos supondo $\mathcal{C}$ irredutível, obtemos

$$\det M = -\frac{ad^2}{4} \neq 0.$$

Aplicando a projetividade $X \to dX$, $Y \to -adY$ e $Z \to Z$ obtemos

$$\tilde{F}(X,Y,Z) = \frac{1}{ad^2}\bar{F}(X,Y,Z) = X^2 + b'Z^2 + c'XZ - YZ$$

e isto torna-se

$$\tilde{\tilde{F}}(X,Y,Z) = X^2 - YZ$$

se aplicarmos a projetividade $X \to X$, $Y \to c'X + Y + b'Z$ e $Z \to Z$. □

E para a cônica $X^2 - YZ = 0$, definida sobre qualquer corpo, temos

Teorema 2.1.4 *Seja $\mathcal{C}$ a cônica irredutível dada por $G(X,Y,Z) = X^2 - YZ$. Então*

$$\mathcal{C}_{|_K} \simeq_K \mathbb{P}^1_K.$$

Prova: Definamos o seguinte mapa:

$$\begin{array}{ccc} \Psi : \mathcal{C} & \dashrightarrow & \mathbb{P}^1 \\ (0:1:0) \neq P = (X:Y:Z) & \longmapsto & \Psi(P) = (X:Z) \end{array}.$$

Ψ é um mapa racional, a projeção de C do ponto $(0:1:0)$ sobre a reta de equação $Y = 0$. Sendo $\mathcal{C}$ uma cônica a reta por P e $(0:1:0)$ corta transversalmente $\mathcal{C} \setminus (0:1:0)$ num único ponto: P. Portanto Ψ é birracional e se estende a um morfismo sobre $\mathcal{C}$ associando a $(0:1:0)$ o ponto $(1:0)$, interseção da reta tangente a $\mathcal{C}$ em $(0:1:0)$ com a reta $Y = 0$. Como Ψ é um morfismo birracional entre curvas lisas, então Ψ é um isomorfismo, cuja inversa é o morfismo

$$\begin{array}{ccc} \Phi : \mathbb{P}^1 & \longrightarrow & \mathcal{C} \\ Q = (S:T) & \longmapsto & \Phi(Q) = (ST : S^2 : T^2) \end{array}.$$

□

Lembremos que uma curva $\mathcal{C}/K$ é dita *curva racional sobre* K se, sobre K, ela for birracional a $\mathbb{P}^1_K$. Assim, da união destes dois resultados obtemos

Corolário 2.1.5 *Uma cônica lisa é uma curva racional sobre K se, e somente se, $\mathcal{C}(K) \neq \emptyset$.* □

Em outras palavras, se quisermos saber se uma cônica lisa $\mathcal{C}_{|_K}$ é uma curva racional sobre K devemos exibir um ponto P *sobre* K, isto é, mostrar que $\mathcal{C}(K) \neq \emptyset$, e este é um fato determinante, como mostram os exemplos abaixo.

Para estes exemplos, consideremos $K = \mathbb{R}$.

Como vimos, uma cônica será projetivamente equivalente a uma cônica do tipo $F(X_0, X_1, X_2) = b_0X_0^2 + b_1X_1^2$ ou $F(X_0, X_1, X_2) = b_0X_0^2 + b_1X_1^2 + b_2X_2^2$. Caso um dos b_i's for negativo, fazendo transformações do tipo $X_i' = \sqrt{-b_i}X_i$ e $X_j' = X_j$, para

$j \neq i$, teremos que estas equações são equivalentes a uma das seguintes:

$$\begin{aligned}
\mathcal{C}_1 &: X_0^2 + X_1^2 = 0 \\
\mathcal{C}_2 &: X_0^2 - X_1^2 = 0 \\
\mathcal{C}_3 &: X_0^2 + X_1^2 - X_2^2 = X_0^2 + (X_1 + X_2)(X_1 - X_2) = {X'}_0^2 + {X'}_1 X_2' = 0 \\
\mathcal{C}_4 &: X_0^2 + X_1^2 + X_2^2 = 0.
\end{aligned}$$

Neste caso encontramos $\mathcal{C}_1 = (0 : 0 : 1)$; $\mathcal{C}_2$ é um par de retas reais; $\mathcal{C}_3$ é uma curva racional sobre $\mathbb{R}$; enquanto que $\mathcal{C}_4$ é uma curva lisa que não é racional sobre $\mathbb{R}$, justamente porque $\mathcal{C}_4(\mathbb{R}) = \emptyset$.

Além disso, das contas feitas acima, podemos concluir o seguinte fato de caráter geral: para uma cônica redutível $\mathcal{C}_{|_K}$, sempre teremos $\mathcal{C}(K) \neq \emptyset$, para qualquer corpo K, embora $\mathcal{C}(K)$ consista de apenas um ponto ou $\mathcal{C}(K)$ seja a união de duas cópias de $\mathbb{P}^1_K$.

E finalmente chegamos ao resultado principal desta seção.

Teorema 2.1.6 *Seja $\mathcal{C}/K$ uma curva lisa de gênero zero. Então $\mathcal{C}$ é isomorfa sobre K a uma cônica lisa.*
Prova: Consideremos o divisor canônico $K_{\mathcal{C}}$ da curva $\mathcal{C}$, que está definido sobre K. Pelo Riemann-Roch (**1.5.4**, pg. 22) temos que $\deg(K_{\mathcal{C}}) = 2g - 2 = -2$ e portanto

$$\deg(-K_{\mathcal{C}}) = 2.$$

Logo, por (**1.5.4**, pg. 22)

$$\ell(-K_{\mathcal{C}}) = \deg(-K_{\mathcal{C}}) - g + 1 = 3$$

Consideremos o mapa $\phi = \phi_{-K_{\mathcal{C}}}$ associado ao divisor $-K_{\mathcal{C}}$. Seja $E = \phi(\mathcal{C})$. Como ϕ é não constante, E é uma curva irredutível de grau pelo menos 2. Pela fórmula do grau do divisor (**1.3.2**, pg. 18) temos

$$2 = \deg(-K_C) = \deg\phi \deg E \geq 2.$$

Portanto $\deg\phi = 1$, $\deg E = 2$, E é lisa (**2.1.2**, pg. 28) e ϕ é um isomorfismo, pois é um mapa birracional entre curvas lisas (**1.2.1**, pg. 12). □

Corolário 2.1.7 *Seja $\mathcal{C}/K$ uma curva lisa de gênero 0.*
(i) $\mathcal{C}$ é isomorfa sobre K a uma cônica em $\mathbb{P}^2$.
(ii) $\mathcal{C}$ é racional se, e somente se, $\mathcal{C}(K) \neq \emptyset$. □

2.2 Cônicas sobre $\mathbb{Q}$ - Princípio Local-Global

Na seção anterior reduzimos o estudos das cônicas projetivas definida sobre $\mathbb{Q}$ a decidir quando uma determinada cônica tem ou não um ponto sobre $\mathbb{Q}$. O teorema de Hasse-Minkowski, chamado às vezes de princípio local-global para cônicas e cujo enunciado e demonstração será visto adiante, fornece uma resposta satisfatória a esta pergunta.

Na prova do princípio local-global usaremos sem demonstração o seguinte resultado devido a Minkowski:

Teorema 2.2.1 (Lema de Minkowski sobre sólidos convexos) *Seja Λ um subgrupo de $\mathbb{Z}^n$ de índice m. Seja $\mathcal{C} \subset \mathbb{R}$ um conjunto convexo e simétrico de volume*

$$V(\mathcal{C}) > 2^n m$$

Então existe $\mathbf{c} \in \mathcal{C} \cap \Lambda$ com $\mathbf{c} \neq \mathbf{0}$.
Prova: [CASSELS], pg. 18. □

Teorema 2.2.2 (Hasse-Minkowski) *Uma condição necessária e suficiente para a existência de um ponto racional sobre uma cônica $\mathcal{C}$ definida sobre $\mathbb{Q}$ é que exista um ponto em $\mathbb{R}$ e um ponto em $\mathbb{Q}_p$, para todo primo $p \geq 2$.*

Em outras palavras, seja $\mathcal{C}_{|_{\mathbb{Q}}}$ uma cônica sobre $\mathbb{Q}$. Então $\mathcal{C}(\mathbb{Q}) \neq \emptyset$ se, e somente se, $\mathcal{C}(\mathbb{R}) \neq \emptyset$ e $\mathcal{C}(\mathbb{Q}_p) \neq \emptyset$, para todo primo $p \geq 2$.

Prova: A necessidade é trivial. Preocuparemo-nos tão somente com a suficiência. Assim supondo que $\forall p$, primo, exista um ponto $\mathbf{a} = (a_1, a_2, a_3) \neq (0,0,0)$ com $a_j \in \mathbb{Q}_p$ tal que $F(\mathbf{a}) = 0$ e multiplicando este vetor pelo inverso do a_j não nulo de maior módulo, podemos supor que

$$max|a_j|_p = 1 \qquad (*)$$

Como vimos existe uma transformação do tipo

$$T : X_i = \sum_j t_{ij} Y_j$$

com $t_{ij} \in \mathbb{Q}$ e $\det(t_{ij}) \neq 0$, de tal forma que tenhamos

$$F(\mathbf{X}) = f_1 X_1^2 + f_2 X_2^2 + f_3 X_3^2, \text{ com } f_i \in \mathbb{Q}$$

Primeiro façamos algumas mudanças de coordenadas de modo a termos os f_j números inteiros livres de quadrados e cujo produto $f_1 f_2 f_3$ também seja livre de quadrados.

Multiplicando $F(\mathbf{X})$ pelo produto dos denominadores dos f_j poderemos supor que eles pertencem a $\mathbb{Z}$. Além disso se f_1, f_2 e f_3 possuírem um fator comum podemos multiplicar $F(\mathbf{X})$ pelo inverso deste fator para que tenhamos $\text{mdc}(f_1, f_2, f_3) = 1$.

Se um dos f_j for da forma $f_j = t_j^2 f_j^{'}$ poderemos fazer a substituição $X_j \to t_j X_j \quad (t_j \in \mathbb{Q})$ de modo que, sem perda de generalidade, os f_j são livre de quadrados.

Podemos também supor que $f_1 f_2 f_3$ seja livre de quadrados, pois se acontecesse $f_1 f_2 f_3 = t^2 q$, como cada f_j é livre de quadrados e $\text{mdc}(f_1, f_2, f_3) = 1$, devemos ter, digamos, $f_1 = t f_1^{'}$ e $f_2 = t f_2^{'}$. Se multiplicarmos F por t e fizermos a substituição $X_j \to t X_j$, $j = 1, 2$, teremos o $f_1 f_2 f_3$ livre de quadrados.

Deste modo teremos $f_1 f_2 f_3 = 2^\lambda p_1 p_2 ... p_r$, onde $\lambda = 1$ ou 0 e os p_i's são primos ímpares distintos.

Agora consideraremos os seguintes casos:

1. $p \neq 2$ e $p \mid f_1 f_2 f_3$

   Suponha que $p \mid f_1$, logo $p \nmid f_2, f_3$, uma vez que $f_1 f_2 f_3$ é livre de quadrados. Portanto $|f_1 a_1^2|_p < 1$. Agora se $|a_2|_p < 1$ teremos:

   $$|f_3 a_3^2|_p = |f_1 a_1^2 + f_2 a_2^2|_p < 1 \Rightarrow |a_3|_p < 1$$

   Logo

   $$|f_1 a_1^2|_p \leq \text{máx}\{|f_2 a_2^2|_p, |f_3 a_3^2|_p\} \leq p^{-2} \Longrightarrow |a_1| \leq p^{-1} < 1$$

   e isto contradiz $(*)$. Logo $|a_2|_p = |a_3|_p = 1$. E assim

   $$|f_2 a_2^2 + f_3 a_3^2|_p < 1$$

Daí, dividindo pela unidade a_2 deduzimos que existe $r_p \in \mathbb{Z}$ tal que

$$f_2 + r_p^2 f_3 \equiv 0 \mod p$$

2. $p = 2$ e $2 \nmid f_1 f_2 f_3$, ou seja, $2 \nmid f_1, f_2, f_3$.

   Suponhamos que $|a_1|_2, |a_2|_2 < 1$. Daí teríamos:

   $$|f_3 a_3^2|_2 = |f_1 a_1^2 + f_2 a_2^2|_2 \leq \max(|f_1 a_1^2|_2, |f_2 a_2^2|_2) < 1$$

   contrariando o fato de termos pelo menos um dos a_i's como unidade. Assim podemos supor que $|a_2|_2 = 1$. Portanto

   $$1 = |f_2 a_2^2|_2 = |f_1 a_1^2 + f_3 a_3^2|_2 \leq \max(|f_1 a_1^2|_2, |f_3 a_3^2|_2)$$

   Donde concluímos que, por exemplo, $|a_3|_2 = |a_2|_2 = 1$. Logo temos que $|f_2 a_2^2 + f_3 a_3^2|_2 \leq 2^{-1}$. Assim existe um $a \in \mathbb{Z}$ tal que:

   $$f_2 + a^2 f_3 \equiv 0 \mod 4$$

   No entanto temos que $\forall a \in \mathbb{Z}$ ocorre $a^2 \equiv 1$ ou $0 \mod 4$. Não pode ocorrer $a^2 \equiv 0 \mod 4$ pois senão teríamos $0 \equiv f_2 + a^2 f_3 \equiv f_2 \mod 4$, contradizendo o fato de f_2 não ser divisível por 2. Portanto se tem:

   $$f_2 + f_3 \equiv 0 \mod 4$$

3. $p = 2$ e $2 \mid f_1 f_2 f_3$

   Digamos que $2 \mid f_1$ e que $2 \nmid f_2 f_3$. Como $2 \mid f_1$ temos que $|f_1 a_1^2|_2 < |a_1^2|_2 \leq 1$. Se ocorresse $|a_2|_2 < 1$ teríamos:

   $$|a_3^2|_2 = |f_3 a_3^2|_2 = |f_2 a_2^2 + f_1 a_1^2|_2 \leq \max(|f_2 a_2^2|_2, |f_1 a_1^2|_2) < 1$$

   podemos concluir que $|a_2|_2 = |a_3|_2 = 1$. Além disso existem duas possibilidades para a_1: ou $|a_1|_2 = 1$ ou $|a_1|_2 < 1$. No primeiro caso, encontraremos inteiros r_1, r_2 e r_3 de modo que:

   $$0 \equiv f_1 r_1^2 + f_2 r_2^2 + f_3 r_3^2 \equiv f_1 + f_2 + f_3 \mod 8$$

   devido ao fato de termos $a^2 \equiv 1 \mod 8$ para qualquer a ímpar. E disto concluímos que

   $$f_1 + f_2 + f_3 \equiv 0 \mod 8.$$

Caso $|a_1|_2 < 1$ teremos

$$|a_1|_2 \leq 2^{-1} \Longrightarrow |a_1^2|_2 \leq 2^{-2} \Longrightarrow 2^{-3} \geq |f_1 a_1^2|_2 = |f_2 a_2^2 + f_3 a_3^2|_2$$

Donde

$$f_2 + f_3 \equiv 0 \mod 8$$

Assim podemos afirmar que

$$s f_1 + f_2 + f_3 \equiv 0 \mod 8$$

onde $s = 1$ ou 0 dependendo de a_1 ser ou não uma unidade.

Se impusermos a seguinte condição

$$x_3 \equiv r_{p_i} x_2 \mod p_i$$

onde p_i é um dos fatores de $|f_1 f_2 f_3|$ então pelo **CASO 1** teremos

$$\begin{aligned} F(\mathbf{X}) &= f_1 x_1^2 + f_2 x_2^2 + f_3 x_3^2 \\ &\equiv (f_2 + r_{p_i}^2 f_3) x_2^2 \equiv 0 \mod p_i \end{aligned}$$

Se por acaso 2 não é fator de $f_1 f_2 f_3$, impondo as condições

$$\begin{cases} x_1 \equiv 0 \mod 2 \\ x_2 \equiv x_3 \mod 2 \end{cases}$$

e utilizando o **CASO 2** teremos

$$F(\mathbf{X}) \equiv 0 \mod 4$$

E de maneira semelhante se $2 \mid f_1 f_2 f_3$ e $2 \mid f_1$, impondo

$$\begin{cases} x_2 \equiv x_3 \mod 4 \\ x_1 \equiv s x_3 \mod 2, \quad \text{onde s} = 1 \text{ ou } 0 \end{cases}$$

e utilizando o **CASO 3** temos

$$F(\mathbf{X}) \equiv 0 \mod 8$$

Consideremos como Λ um dos seguintes subgrupos de $\mathbb{Z}^3$

$$\begin{cases} x_3 \equiv r_{p_i} x_2 \mod p_i, \ \forall i \\ x_1 \equiv 0 \mod 2 \\ x_2 \equiv x_3 \mod 2 \end{cases} \quad \text{ou} \quad \begin{cases} x_3 \equiv r_{p_i} x_2 \mod p_i, \ \forall i \\ x_1 \equiv s x_3 \mod 2 \\ x_2 \equiv x_3 \mod 4 \end{cases}$$

O primeiro será considerado caso $2 \nmid f_1 f_2 f_3$ enquanto que tomaremos o segundo se $2 \mid f_1 f_2 f_3$.

Em qualquer um dos casos, sempre obtemos $\forall \mathbf{X} \in \Lambda$

$$F(\mathbf{X}) \equiv 0 \mod 4|f_1 f_2 f_3|$$

AFIRMAÇÃO : O subgrupo Λ tem índice $m = 4|f_1 f_2 f_3|$

Consideremos agora o seguinte conjunto convexo e simétrico

$$\mathcal{C} : |f_1| x_1^2 + |f_2| x_2^2 + |f_3| x_3^2 < 4|f_1 f_2 f_3|$$

ou

$$\mathcal{C} : \frac{|f_1|}{4|f_1 f_2 f_3|} x_1^2 + \frac{|f_2|}{4|f_1 f_2 f_3|} {x_2}^2 + \frac{|f_3|}{4|f_1 f_2 f_3|} x_3^2 < 1$$

que é um sólido limitado por um elipsóide ε e cujo volume é dado por

$$V(\mathcal{C}) = \frac{4}{3}\pi \sqrt{4 f_1 f_2} \sqrt{4 f_1 f_3} \sqrt{4 f_2 f_3} = \frac{4}{3}\pi 2^3 |f_1 f_2 f_3| > 2^3 |4 f_1 f_2 f_3| \geq 2^3 m$$

Portanto, pelo teorema de Minkowski, existe um $\mathbf{0} \neq \mathbf{c} \in \Lambda \cap \mathcal{C}$. Para este $\mathbf{c}$ temos

$$\begin{cases} F(\mathbf{c}) \equiv 0 \mod 4|f_1 f_2 f_3| \\ |F(\mathbf{c})| \leq |f_1| c_1^2 + |f_2| c_2^2 + |f_3| c_3^2 < 4|f_1 f_2 f_3| \end{cases}$$

Logo

$$F(\mathbf{c}) = 0$$

e portanto concluímos a demonstração do teorema.

Para demonstrar a afirmação consideremos, inicialmente, os subgrupos de $\mathbb{Z}^3$, $\Lambda_i : x_3 \equiv r_{p_i} x_2 \mod p_i$, e os seguintes homomorfismos $g_i : \mathbb{Z}^3 \to \dfrac{\mathbb{Z}}{p_i \mathbb{Z}}$ definido por

$$(x_1, x_2, x_3) \longmapsto \overline{x_3 - r_{p_i} x_2}.$$

Cada g_i é sobrejetivo, pois sempre podemos encontrar soluções inteiras para a equação $x_3 - r_{p_i} x_2 = d$, $\forall d \in \mathbb{Z}$. Ademais, $\ker g_i = \Lambda_i$ donde

$$\frac{\mathbb{Z}^3}{\Lambda_i} \simeq \frac{\mathbb{Z}}{p_i\mathbb{Z}} \qquad \text{e} \qquad [\mathbb{Z}^3 : \Lambda_i] = p_i$$

Chamemos de Γ_1 ao subgrupo

$$\begin{cases} x_1 \equiv 0 \mod 2 \\ x_2 \equiv x_3 \mod 2 \end{cases}$$

Para Γ_1 conseguimos um homomorfismo sobrejetivo $h_1 : \mathbb{Z}^3 \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ definido por

$$(x_1, x_2, x_3) \longmapsto (\overline{x_1}, \overline{x_2 - x_3}).$$

O núcleo de h_1 é o subgrupo Γ_1; portanto

$$\frac{\mathbb{Z}^3}{\Gamma_1} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \qquad \text{e} \qquad [\mathbb{Z}^3 : \Gamma_1] = 4$$

Com considerações semelhantes constrói-se a seguinte seqüencia exata de grupos

$$0 \to \Gamma_2 \to \mathbb{Z}^3 \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \to 0$$

mostrando que

$$[\mathbb{Z}^3 : \Gamma_2] = 8$$

onde

$$\Gamma_2 : \begin{cases} x_2 \equiv x_3 \mod 4 \\ x_1 \equiv s x_3 \mod 2, \quad \text{onde s = 1 ou 0.} \end{cases}$$

É fácil mostrar que $\Lambda_i + \Gamma_1 = \mathbb{Z}^3$, $\Lambda_i + \Gamma_2 = \mathbb{Z}^3$ e $\Lambda_i + \Lambda_j = \mathbb{Z}^3$, $\forall i \neq j$.

Definiremos o seguinte mapa sobrejetivo

$$\begin{array}{rcl} \phi_t : \mathbb{Z}^3 & \longrightarrow & (\prod_i \dfrac{\mathbb{Z}^3}{\Lambda_i}) \times \dfrac{\mathbb{Z}^3}{\Gamma_t} \\ \mathbf{x} = (x_1, x_2, x_3) & \longmapsto & \phi(\mathbf{x}) = ([\mathbf{x}], ..., [\mathbf{x}]). \end{array}$$

onde $t = 1, 2$ e $[\mathbf{x}]$ indica a classe de $\mathbf{x}$ módulo o respectivo subgrupo.

Pelo teorema do resto chinês temos que $\ker \phi_t = (\bigcap_i \Lambda_i) \bigcap \Gamma_t = \Lambda$. Portanto $\frac{\mathbb{Z}^3}{\Lambda} \simeq \prod_i (\frac{\mathbb{Z}^3}{\Lambda_i}) \times \frac{\mathbb{Z}^3}{\Gamma_t}$.

Quando $t = 1$, ou seja, se $2 \nmid f_1 f_2 f_3$ teremos

$$\begin{aligned} [\mathbb{Z}^3 : \Lambda] &= [\mathbb{Z}^3 : \prod_i (\frac{\mathbb{Z}^3}{\Lambda_i}) \times \frac{\mathbb{Z}^3}{\Gamma_1}] \\ &= (\prod_i [\mathbb{Z}^3 : (\frac{\mathbb{Z}^3}{\Lambda_i})])[\mathbb{Z}^3 : \frac{\mathbb{Z}^3}{\Gamma_1}] \\ &= 4(\prod_i p_i) = 4|f_1 f_2 f_3|. \end{aligned}$$

Para $t = 2$, isto é, quando $2 \mid f_1 f_2 f_3$ e $2 \mid f_1$, teremos

$$\begin{aligned} [\mathbb{Z}^3 : \Lambda] &= [\mathbb{Z}^3 : \prod_i (\frac{\mathbb{Z}^3}{\Lambda_i}) \times \frac{\mathbb{Z}^3}{\Gamma_2}] \\ &= (\prod_i [\mathbb{Z}^3 : (\frac{\mathbb{Z}^3}{\Lambda_i})])[\mathbb{Z}^3 : \frac{\mathbb{Z}^3}{\Gamma_2}] \\ &= (\prod_i p_i)8 = 4(2\prod_i p_i) \\ &= 4|f_1 f_2 f_3|. \end{aligned}$$

□

Dentro deste teorema mostramos que se uma cônica dada por $f_0 X_0^2 + f_1 X_1^2 + f_2 X_2^2$ tiver soluções locais então os coeficientes satisfazem

- $p | f_1 f_2 f_3$ e $p \neq 2$. Neste caso existe $r_p \in \mathbb{Z}$ tal que

  $$f_2 + r_p^2 f_3 \equiv 0 \mod p \quad \text{ou} \quad f_1 + r_p^2 f_3 \equiv 0 \mod p \quad \text{ou} \quad f_1 + r_p^2 f_2 \equiv 0 \mod p$$

  a depender de termos $p \mid f_1$, $p \mid f_2$ ou $p \mid f_3$, respectivamente.

- $2 \nmid f_1 f_2 f_3$. Então

  $$f_2 + f_3 \equiv 0 \mod 4$$

- $2|f_1f_2f_3$. Caso $2 \mid f_1$, conseguimos

$$f_1 + f_2 + f_3 \equiv 0 \mod 8 \text{ ou } f_2 + f_3 \equiv 0 \mod 8$$

  Valem congruências semelhantes, para $2 \mid f_2$ ou $2 \mid f_3$.

Usando uma das formas do lema de Hensel (ver próxima seção) se a cônica possuir uma solução em $\mathbb{R}$ mostra-se que a recíproca deste fato é verdadeira, gerando uma maneira efetiva de mostrar a existência de pontos com coordenadas racionais numa cônica.

Exemplo 2.1 $2X^2 + 17Y^2 - Z^2 = 0$.

O produto dos coeficientes é divisível por 2 e 17. Renumerando os coeficientes de uma maneira conveniente, para $p = 17$ devemos verificar a existência de uma solução para

$$x^2 \equiv 2 \mod 17,$$

ou seja, verificar se 2 é um resíduo quadrático módulo 17, o que é facilmente feito usando o critério de Euler.

Como o produto dos coeficientes é par e claramente

$$17 - 1 \equiv 0 \mod 8,$$

a cônica satisfaz todas as condiçoẽs, possuindo assim uma solução racional, a saber $(2, 1, 5)$.

2.3 Contra exemplo para o princípio Local-Global

Vimos o quanto é importante a existência de um ponto racional sobre uma cônica para podermos obter sua real estrutura. Entretanto, mostraremos aqui, que para curvas de grau maior ou igual a 3, o princípio local-global (PLG) não se aplica e se quisermos determinar um ponto racional sobre a curva, deveremos produzir um novo método.

O mais famoso contra-exemplo para o PLG é a curva

$$3X^3 + 4Y^3 + 5Z^3 = 0$$

que Selmer mostrou possuir soluções locais sem possuir soluções globais (veja, por exemplo, [CASSELS], pg. 87).

A curva que mostraremos não satisfazer o PLG é

$$X^4 - 17 = 2Y^2$$

e foi obtida independentemente por Lind e Reichardt.

Começaremos pelas soluções locais. Para isso usaremos o seguinte resultado

Teorema 2.3.1 (Lema de Hensel) *Sejam $f(X) \in \mathbb{Z}_p[X]$ um polinômio e $f'(X)$ sua derivada formal. Suponha que exista um $a_1 \in \mathbb{Z}_p$ tal que*

$$|f(a_1)|_p < |f'(a_1)|_p^2.$$

Então existe $a \in \mathbb{Z}_p$ tal que

$$f(a) = 0 \qquad e \qquad |a - a_1|_p \leq \left| \frac{f(a_1)}{f'(a_1)^2} \right|_p < 1$$

Prova: [GOUVÊA], pg. 70 □

Corolário 2.3.2 *Seja $F(X_1, ..., X_n) \in \mathbb{Z}_p[X_1, ..., X_n]$ e suponha que exista um ponto $(a_1, ..., a_n) \in \mathbb{Z}_p^n$ tal que, para algum i, tenhamos*

$$|F(a_1, ..., a_n)|_p < \left| \frac{\partial F}{\partial X_i}(a_1, ..., a_n) \right|_p^2$$

Então F tem uma raíz em $\mathbb{Z}_p^n$.
Prova: Suponhamos $i = 1$. Considere o polinômio $f(T) = F(T, a_2, ..., a_n)$. Para a_1, f satisfaz

$$|f(a_1)|_p < |f'(a_1)|_p^2.$$

Portanto, pelo lema de Hensel, existe $a \in \mathbb{Z}_p$ tal que

$$F(a, a_2, ..., a_n) = f(a) = 0$$

□

Teorema 2.3.3 *A curva $X^4 - 17 = 2Y^2$ possui solução em $\mathbb{Q}_p$, para todo primo p e para $p = \infty$.*
Prova: Para a curva definida pelo polinômio $F(X, Y) = 2Y^2 - X^4 + 17$ temos $\dfrac{\partial F}{\partial X} = -4X^3$.

Consideremos $Y = p$, $X = p^{-3}$. Neste caso temos

$$\begin{array}{rcll} |2Y^2|_p \leq p^{-3} & < & 1 & \text{(igualdade se } p = 2) \\ |X^4|_p = p^{12} & > & 1 & \\ |17|_p & \leq & 1 & \text{(desigualdade se } p = 17) \\ |4X^3|_p^2 & \geq & p^{14} & \text{(igualdade se } p = 2) \end{array}$$

Logo

$$|F(p^{-1}, p^{-3})|_p \leq \text{máx}\{|2Y^2|_p, |X^4|_p, |17|_p\} = p^{12} < p^{14} \leq |4X^3|_p^2 = \left|\frac{\partial F}{\partial X}(p^{-1}, p^{-3})\right|_p^2$$

Daí F tem uma solução em $\mathbb{Z}_p$. □

Teorema 2.3.4 $2Y^2 = X^4 - 17$ *não possui pontos racionais.*
Prova: Suponha que (x, y) é um ponto nesta curva. Suponha $x = \dfrac{a}{c}$ irredutível. Então

$$a^4 - 17c^4 = 2b^2, \qquad \text{mdc}(a, c) = \text{mdc}(a, b) = \text{mdc}(b, c) = 1$$

Colocando $A = a^2$ e $C = c^2$ temos

$$A^2 - 17C^2 = 2b^2$$

Esta equação possui uma solução racional já que possui soluções locais, veja (**2.1**, pg. 39).

Temos

$$\begin{array}{rcl} (5A + 17C + 4b)(5A + 17C - 4b) & = & (5A + 17C)^2 - (4b)^2 \\ & = & 25A^2 + 2 \cdot 5 \cdot 17AC + 17^2C^2 - 8(2b^2) \\ & = & 25A^2 + 2 \cdot 5 \cdot 17AC + 17^2C^2 - 8(A^2 - 17C^2) \\ & = & 17A^2 + 2 \cdot 5 \cdot 17AC + 17(17 + 8)C^2 \\ & = & 17(A + 5C)^2 \end{array}$$

Se existir um divisor primo ímpar q comum aos dois fatores do primeiro membro da igualdade acima teríamos

$$\begin{aligned} q \mid 2(5A+17C) &= (5A+17C+4b)+(5A+17C-4b) \\ q^2 \mid 17(A+5C) &= (5A+17C+4b)(5A+17C-4b) \\ q \mid 8A &= 5(5A+17C)-17(A+5C) \\ q \mid 8C &= -(5A+17C)+5(A+5C) \end{aligned}$$

Os dois fatores devem ter sinais iguais já que seu produto é um número positivo, e lembrando que $A = a^2$ e $C = c^2$ vemos que o sinal deve ser positivo. Portanto, pela fatoração única, deve existir inteiros u e v tais que vale uma das possibilidades

	Caso 1	Caso 2
$5a^2+17c^2 \pm 4b =$	$17u^2$	$34u^2$
$5a^2+17c^2 \pm 4b =$	v^2	$2v^2$
$a^2+5c^2 =$	uv	$2uv$

No primeiro caso, ao somarmos as duas primeiras equações , obtemos

$$\begin{aligned} 10a^2+34c^2 &= 17u^2+v^2 \\ a^2+5c^2 &= uv \end{aligned}$$

Esta primeira equação módulo 17 é

$$10a^2 \equiv v^2 \mod 17$$

e como 10 não é um quadrado em $\mathbb{Z}/17\mathbb{Z}$ devemos ter que 17 divide a e v. Se isto ocorre, ao olharmos a segunda equação acima temos que 17 divide c, absurdo pois $\text{mdc}(a,c) = 1$.

O segundo caso fornece-nos as equações

$$\begin{aligned} 5a^2+17c^2 &= 17u^2+v^2 \\ a^2+5c^2 &= 2uv \end{aligned}$$

Olhando esta equação em $\mathbb{Z}/17\mathbb{Z}$ e fazendo considerações semelhantes as anteriores levam a uma contradição. □

2.4 Cônicas sobre corpos finitos

Seja $k = \mathbb{F}_q$, com $q = p^r, p$: primo, o corpo com q elementos. Notemos que o grupo multiplicativo $\mathbb{F}_q^*$ é cíclico de ordem $q-1$, [SERRE], pg. 4.

Seja $u \geq 0$ um inteiro. Seja $f(\mathbf{X}) = f(X_1, ..., X_n) \in k[\mathbf{X}] = k[X_1, ..., X_n]$ e considere a seguinte soma $S(f) = \sum_{\mathbf{x} \in k^n} f(\mathbf{x})$. Nestas condições temos:

Lema 2.4.1

$$S(X^u) = \sum_{x \in k} x^u = \begin{cases} -1 & \textit{se } u \geq 1 \textit{ e } (q-1) \mid u \\ 0 & \textit{caso contrário.} \end{cases}$$

Prova: Para $u = 0$ temos

$$S(x^0) = S(1) = \sum_{x \in k} 1 = q \cdot 1 = 0$$

já que k tem característica p e também consideramos que $0^0 = 1$.

Se $u > 0$ e u é divisível por $q-1$, digamos $u = (q-1)m$, teremos $0^u = 0$ e $x^u = (x^{q-1})^m = 1^m = 1$, para todo $x \neq 0$. Daí

$$S(X^u) = (q-1) \cdot 1 + 0 = q \cdot 1 - 1 = -1.$$

Por outro lado, se $u > 0$ e $q-1$ não divide u, existirá um $y \in k^*$ tal que $y^u \neq 1$, basta lembrarmos que k^*, como observamos anteriormente, é um grupo cíclico de ordem $q-1$. Note ainda que $k = \{yx \mid x \in k\}$, pois k é finito e $yx = yz \Rightarrow x = z$. Sendo assim

$$S(X^u) = \sum_{x \in k} x^u = \sum_{x \in k} (xy)^u = \sum_{x \in k} x^u y^u = y^u (\sum_{x \in k} x^u) = y^u (S(X^u))$$

donde

$$(1 - y^u) S(X^u) = 0 \Rightarrow S(X^u) = 0.$$

□

Teorema 2.4.2 (Chevalley-Warning) - *Sejam* $f_\alpha \in k[X_1, ..., X_n]$ *tais que* $\sum_\alpha \deg f_\alpha < n$ *e considere* $V = \{\mathbf{v} = (v_1, ..., v_n) \in \mathbb{A}^n(k) \mid f_\alpha(\mathbf{v}) = 0, \forall \alpha\}$.
Então $\text{card}(V) \equiv 0 \mod p$.

Prova: Ponha $P(x) = \prod_\alpha (1 - {f_\alpha}^{q-1}(x))$. Se $x \in V$, temos que $f_\alpha(x) = 0, \forall \alpha$. Daí $P(x) = 1$. Caso $x \notin V$ teremos $f_\alpha(x) \neq 0$, ou seja, ${f_\alpha}^{q-1}(x) = 1$, portanto $P(x) = 0$. Assim

$$S(P) = \sum_{x \in k} P(x) = \sum_{x \in V} 1 + \sum_{x \notin V} 0 = \text{card}(V) \cdot 1.$$

Daí se pudermos mostrar que $0 = S(P) = \text{card}(V) \cdot 1$ teremos o resultado desejado, i.e., $\text{card}(V) \equiv 0 \mod p$

Por hipótese $\sum_\alpha \deg f_\alpha < n$. Logo

$$\begin{aligned} \deg P &= \deg \prod_\alpha (1 - f_\alpha^{q-1}) \\ &= \sum_\alpha \deg(1 - f_\alpha^{q-1}) \\ &= \sum_\alpha \deg(f_\alpha^{q-1}) \\ &= (q-1)(\sum_\alpha deg f_\alpha) < n(q-1) \end{aligned}$$

portanto todos os monômios de P são da seguinte forma $X_1^{u_1}...X_n^{u_n}$, com $\sum u_i < n(q-1)$ e, claramente, pelo menos um dos u_i é menor que $q-1$. Portanto

$$S(X_1^{u_1}...X_n^{u_n}) = \sum_{(x_1,...,x_n) \in \mathbb{A}_k^n} x_1^{u_1}...x_n^{u_n} = \prod_i (\sum_{x_i \in k} x_i^{u_i})$$

Usando o lema, vemos que esta soma é igual a zero uma vez que um dos $u_i < q-1$, logo não divisível por $q-1$. Para finalizar, observe apenas que $S(P)$ é uma combinação linear de somas deste tipo. Assim segue o resultado. □

Como corolário imediato teremos

Corolário 2.4.3 *Sejam* f_α *polinômios em* $k[X_1, ..., X_n]$ *tais que* $\sum \deg f_\alpha < n$ *e sem termo constante. Então os* f_α *tem uma solução comum não nula.*

Prova: De fato, se a única solução fosse a trivial teríamos que $\text{card}(V(\{f_\alpha\})) = 1$ que certamente não é divisível por p. □

Aplicando este corolário para cônicas temos

Corolário 2.4.4 *Toda cônica projetiva sobre um corpo finito tem uma solução (não trivial).* □

Corolário 2.4.5 *Toda curva lisa e irredutível de gênero zero sobre um corpo finito $\mathbb{F}_q$ é isomorfa sobre $\mathbb{F}_q$ a $\mathbb{P}^1_{\mathbb{F}_q}$.* □

Corolário 2.4.6 *Toda hipersuperfície projetiva $\mathbf{X} = V(F)$ de $\mathbb{P}^n_k$ de grau $d \leq n$ tem um ponto racional sobre k, isto é, $\mathbf{X}(k) \neq \emptyset$* □

2.5 Cônicas sobre corpos de funções de curvas algébricas

Nesta seção k é um corpo algebricamente fechado.

Teorema 2.5.1 (Tsen) - *Seja $K|k$ uma extensão de corpos com grau de transcendência um. Tomemos $f_1, f_2, ..., f_s \in K[X_1, ..., X_n]$ polinômios homogêneos que satisfazem $\sum \deg f_i \leq n$. Então o sistema de equações $f_1 = ... = f_s = 0$ tem uma solução não trivial.*
Prova: Chamemos de S ao corpo gerado sobre k por todos os coeficientes dos f_i. Claramente $f_1, ..., f_s \in S[X_1, ..., X_n] \subset K[X_1, ..., X_n]$. Se $S|k$ é uma extensão algébrica então nada há para mostrar. Caso $S|k$ não seja algébrica então ela deverá ter grau de transcendência um, desta forma nos reduzimos a demonstrar o resultado para extensões finitamente geradas. Assim sendo suponha que $K|k$ é finitamente gerada e tem grau de transcendência um.

Note que qualquer $t \in K - k$ é transcendente, pois k é algebricamente fechado e $\text{gr.tr.}_k K = 1$. Considere, assim, o fecho inteiro $R \subset K$ de $k[t]$ em K. R é um

$k[t]$-módulo livre, já que como $k[t]$-módulo podemos decompô-lo numa soma direta de um $k[t]$-módulo livre e um $k[t]$-módulo de torção. No entanto, R está contido em K, corpo, e não possui torção.

Seja $c_1, ..., c_r$ uma $k[t]$-base para R. Multiplicando todos os c_j's temos:

$$c_i c_j = \sum_p \gamma_{i,j,p} c_p \text{ onde } \gamma_{i,j,p} \in k[t]$$

Ponha $h := \max \deg \gamma_{i,j,p}$.

Se multiplicarmos os f_i por constantes apropriadas, podemos supor que eles têm coeficientes em R. Portanto podemos escrever cada coeficiente $f_{j,J}$ de f_j como:

$$f_{j,J} = \sum_p f_{j,J,p} c_p \text{ onde } f_{j,J,p} \in k[t]$$

Definamos $m := \max \deg f_{j,J,p}$.

Estamos procurando por soluções da forma $x_i = \sum_p u_{i,p} c_p$ onde os $u_{i,p}$ são polinômios em $k[t]$ de grau no máximo d. Se olharmos os coeficientes dos x_i como incógnitas, eles corresponderão a pontos do espaço projetivo de dimensão $r(d+1)(n+1) - 1$.

Vejamos sob quais condições existirá uma solução deste tipo. Para isso escrevamos:

$$f_j(x_0, ..., x_n) = f_j(\sum_p u_{0,p} c_p, ..., \sum_p u_{n,p} c_p) = \sum_p F_{j,p}(t) c_p$$

onde $F_{j,p} \in k[t]$. Notemos que os $F_{j,p}$ são expressões polinomiais dos $u_{i,p}$. Deste modo, se impusermos $f_j(x_0, ..., x_n) = 0$ obteremos $\sum_p (1 + \deg F_{j,p})$ equações , uma para cada coeficiente de $F_{j,p}$, sobre os coeficientes de $u_{i,p}$. Expandindo $f_j(x_0, ..., x_n)$ obteremos os $F_{j,p}$ como termos que possuem a seguinte forma:

$$(f_{j,J} \prod_{1 \leq s \leq \deg f_j} c_{p_s})(\prod_{1 \leq s \leq \deg f_j} u_{i_s,k_s})$$

O grau da última parcela desta expressão é $\sum_{s=1}^{\deg f_j} u_{i_s,p_s} \leq \sum_{s=1}^{\deg f_j} d = d \deg f_j$, já que os $u_{i,p}$ tem grau no máximo d. Cálculo semelhante mostra que o grau da primeira

parcela é no máximo $h \deg f_j + m$. Daí $\deg F_{j,p} \leq (d+h)\deg f_j + m$. Portanto o número total de equações será no máximo:

$$\begin{aligned}\sum_{p=1}^{r}(1+F_{j,p}) &\leq \sum_{p=1}^{r}(1+(d+h)\deg f_j + m) \leq r(\sum_{j}(d+h)\deg f_j + m + 1) \\ &\leq r(n(d+h)+m+1)\end{aligned}$$

Se tomarmos soluções x_i cujo grau d satisfaça $d > hn + m - n + \frac{1}{r}$ teremos:

$$\begin{aligned}rd > rh + rm - rn + 1 &\implies rnd + rd > rhn + rnd + rm - rn + 1 \implies \\ &\implies rnd + rd + rn + r > rnd + rh + rm + r + 1 \implies \\ &\implies rd(n+1) + r(n+1) - 1 > rn(d+h) + rm + r \implies \\ &\implies r(d+1)(n+1) - 1 > r(n(d+h)+m+1) \geq \\ &\geq \sum_{p=1}^{r}(1+F_{j,p})\end{aligned}$$

Logo teremos um sistema com menos equações do que a dimensão do espaço projetivo, então este sistema terá uma solução não trivial, já que o corpo k é algebricamente fechado. □

Corolário 2.5.2 *Seja $\mathcal{C}_{|_K} \subset \mathbb{P}^2_K$ uma cônica, com K um corpo de funções de uma curva algébrica definida sobre $k = \bar{k}$. Então $\mathcal{C}(K) \neq \emptyset$ e portanto $\mathcal{C} \cong \mathbb{P}^1_K$.*

Corolário 2.5.3 *Seja $\mathcal{C}_{|_K}$, K como acima, uma curva lisa de gênero 0 definida sobre K, então $\mathcal{C}_{|_K} \cong \mathbb{P}^1_K$.*

Capítulo 3

Curvas Elípticas

3.1 Definição e propriedades iniciais

Definição 3.1 *Uma curva elíptica sobre K é um par (E, O), onde E é uma curva lisa de gênero 1 definida sobre K e $O \in E(K)$.*

Muitas vezes ao nos referirmos a uma curva elíptica E não especificaremos o ponto O, deixando implícito a sua existência. Chamaremos o ponto O de *ponto base* da curva elíptica E ou ainda de *elemento neutro* desta curva. Note que devido ao exemplo de Selmer, a curva definida por $3X^3 + 4Y^3 + 5z^3$, a existência de um ponto racional é extremamente importante.

Vejamos que tipos de propriedades uma curva deste tipo pode ter.

Teorema 3.1.1 *Seja E uma curva elíptica definida sobre K.*
(1) Existem funções $x, y \in K(E)$ tais que o mapa

$$\begin{array}{ccc} \phi : E & \longrightarrow & \mathbb{P}^2_K \\ P & \longmapsto & \phi(P) = (x(P) : y(P) : 1) \end{array}$$

é um isomorfismo definido sobre K de E/K sobre uma curva plana de equação:

$$\mathcal{C} : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

com $a_1, a_2, a_3, a_4, a_6 \in K$ e $\phi(O) = (0 : 1 : 0)$(Mais adiante esclareceremos o porquê desta numeração dos coeficientes).

(2) Reciprocamente, toda curva plana lisa $\mathcal{C}$ dada por uma equação polinomial como a anterior é uma curva elíptica definida sobre K com $O = (0 : 1 : 0) \in C(K)$, seu ponto base.

Prova: (1) Consideremos os espaços vetoriais $\mathcal{L}(n(O))$ para $n = 1, 2, ...$

Como $\deg(n(0)) = n > 0 = 2g - 2$, pelo teorema de Riemann-Roch (**1.5.3**, pg. 21) teremos que $\forall n \geq 1$:

$$\ell(n(O)) = \dim_k \mathcal{L}(n(O)) = \deg(n(O)) - g + 1 = n$$

Desta forma podemos escolher funções $x, y \in K(E)$, conforme (**1.5.8**, pg. 25) de forma que $\{1, x\}$ forme uma base para $\mathcal{L}(2(O)) \subset \mathcal{L}(3(O))$ e $\{1, x, y\}$ seja uma base para $\mathcal{L}(3(O))$. Se x tivesse um pólo em O de ordem < 2, então $x \in \mathcal{L}((O)) = K$ e $\{1, x\}$ seriam linearmente dependentes. Logo $\mathrm{ord}_O\, x = -2$. Analogamente, mostra-se que y é uma função que tem em O um pólo de ordem 3.

Seja t um paramêtro local para E no ponto O. Portanto , existem $u_x, u_y \in K(E)$ tais que $u_x(O) \neq 0$ e $u_y(O) \neq 0$, $x = u_x t^{-2}$ e $y = u_y t^{-3}$. Desta forma, teremos que $\mathrm{ord}_O\, x^2 = -4$, $\mathrm{ord}_O\, xy = -5$, $\mathrm{ord}_O\, x^3 = -6$ e $\mathrm{ord}_O\, y^2 = -6$, mostrando assim que $1, x, y, xy, x^2, x^3, y^2 \in \mathcal{L}(6(O))$.

Como $\ell(6(O)) = 6$, teremos que para estas sete funções existe uma relação de dependência linear entre elas, digamos:

$$A_1 + A_2 x + A_3 y + A_4 x^2 + A_5 xy + A_6 y^2 + A_7 x^3 = 0$$

com os $A_j \in K$ e um deles não nulo.

Além disso se ocorresse que $A_7 A_6 = 0$ teríamos que $A_1 + A_2 x + A_3 y + A_4 x^2 + A_5 xy + A_6 y^2 = 0$ ou $A_1 + A_2 x + A_3 y + A_4 x^2 + A_5 xy + A_7 x^3 = 0$ seria uma relação de dependência linear entre elementos de ordem diferentes. No entanto estes elementos de ordem diferentes são linearmente independentes em $\mathcal{L}(6(O))$. Portanto, $A_6 A_7 \neq 0$, ou seja, nesta combinação linear x^3 e y^2 devem figurar.

Fazendo as substituições $x \to -A_6 A_7 x$ e $y \to A_6 A_7^2 y$ temos:

$$A_1 - A_2 A_6 A_7 x + A_4 A_6^2 A_7^2 x^2 - A_6^3 A_7^4 x^3 + A_3 A_6 A_7^2 y - A_4 A_6^2 A_7^3 xy + A_6^3 A_7^4 y^2 = 0$$

que quando dividida por $A_6^3 A_7^4$ nos dá a equação desejada.

O mapa $\phi : E \to \mathbb{P}^2$ definido por $\phi = (x : y : 1)$ tem imagem contida na curva $\mathcal{C}$ dada pela equação acima. Note ainda que $\phi : E \to \mathcal{C} \subset \mathbb{P}^2$ é um morfismo

sobrejetivo pois é um mapa racional não constante de uma curva lisa para uma variedade projetiva (**1.2.1**, pg. 12). Usando a representação de x e y em termos do paramêtro local da curva em O vemos que

$$\phi = (x : y : 1) = (u_x t^{-2} : u_y t^{-3} : 1) = (u_x t : u_y : t^{-3}).$$

Portanto teremos:

$$\phi(O) = (u_x(O)t(O) : u_y(O) : [t(O)]^3) = (0 : 1 : 0)$$

pois $t(O) = 0$ e $u_y(O) \neq 0$, já que t é um paramêtro local e u_y é uma unidade em $\mathcal{O}_O$.

ϕ será um isomorfismo se mostrarmos que ϕ tem grau 1 e que C é não singular(**1.2.6**, pg. 14).

Mostrar que ϕ tem grau 1 é, por definição, mostrar que $[K(x, y) : K(E)] = 1$, já que $K(\mathcal{C}) = K(x, y)$. Em outras palavras, queremos que $K(E) = K(x, y)$.

Como $x \in \mathcal{L}(2(O))$ podemos concluir que o único pólo de x é O, que como vimos anteriormente tem ordem 2. Definamos o seguinte mapa $\mathbf{x} : E \to \mathbb{P}^1$ dado por:

$$\begin{cases} (x(P) : 1) & \text{se } x \text{ é regular em } P, \\ (1 : 0) & \text{caso } P = O. \end{cases}$$

Deste modo $\mathbf{x}^{-1}(1 : 0) = \{O\}$. E daí, por (**1.2.7**, pg. 15),

$$2 = e_{\mathbf{x}}(O) = \sum_{P \in \mathbf{x}^{-1}(1:0)} e_{\mathbf{x}}(P) = \deg \mathbf{x}$$

Logo $[K(E) : K(x)] = 2$.

Similarmente, mostramos que o mapa $\mathbf{y} = (y : 1) : E \to \mathbb{P}^1$ tem grau 3 e que, portanto, $[K(E) : K(y)] = 3$. Como

$$3 = [K(E) : K(y)] = [K(E) : K(x, y)][K(x, y) : K(y)]$$

e

$$2 = [K(E) : K(x)] = [K(E) : K(x, y)][K(x, y) : K(x)]$$

podemos concluir que $[K(E) : K(x, y)] = 1$ ou equivalentemente, $K(E) = K(x, y)$.

(2) Suponha agora que $\mathcal{C}$ dada pelo polinômio $Y^2+a_1XY+a_3Y = X^3+a_2X^2+a_4X+a_6$ seja singular. Então existe um mapa racional $\psi : \mathcal{C} \dashrightarrow \mathbb{P}^1$ de grau 1 (**3.1.2**, pg. 51).

Daí $\psi \circ \phi : E \to \mathbb{P}^1$ é um mapa de grau 1 entre curvas lisas, portanto por (**1.2.6**, pg. 14) é um isomorfismo. No entanto, E tem gênero 1 enquanto que $\mathbb{P}^1$ tem gênero 0; o que nos dá uma contradição. Logo $\mathcal{C}$ é lisa e ϕ é um isomorfismo.

(2) Se $\mathcal{C}$ é dada por uma curva não singular do tipo

$$\mathcal{C} : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

resta-nos mostrar que $\mathcal{C}$ tem gênero 1, já que $(0:1:0) \in \mathcal{C}(K)$ pode ser o elemento neutro desta curva.

(**1.5.7**, pg. 23) nos diz que para curvas lisas dada por um polinômio homogêneo $F(X,Y,Z) \in K[X,Y,Z]$ de grau d temos

$$g = \frac{(d-1)(d-2)}{2}$$

onde g é o gênero da curva.

Assim nossa curva $\mathcal{C}$ tem gênero $g = \dfrac{(3-1)(3-2)}{2} = 1$. □

Lema 3.1.2 *Seja $\mathcal{C}$ uma curva dada por*

$$Y^3 + a_1XY + a_2Y - X^3 - a_2X^2 - a_4X - a_6 \in K[X,Y].$$

Se $\mathcal{C}$ é singular então existe um mapa racional $\psi : \mathcal{C} \dashrightarrow \mathbb{P}^1$ definido sobre K de grau 1.

Prova: Podemos supor, fazendo $X \to X+a$ e $Y \to Y+b$, que $(0,0)$ é o ponto singular desta curva. Assim:

$$\begin{aligned} a_4 &= \frac{\partial F}{\partial X}(0,0) = 0 \\ a_3 &= \frac{\partial F}{\partial Y}(0,0) = 0 \end{aligned}$$

Logo $\mathcal{C}$ será definida pela equação

$$F : Y^2 + a_1XY = X^3 + a_2X^2$$

Seja então $\psi : \mathcal{C} \dashrightarrow \mathbb{P}^1$ o mapa racional definido por $\psi(x, y) = (x : y)$. Claramente, $\psi^*(K(\mathbb{P}^1)) = K(x, y) = K(\mathcal{C})$; donde $\deg \psi = 1$.

A inversa racional de ψ é

$$\begin{array}{ccc} \mathbb{P}^1 & \longrightarrow & E \\ (1 : t) & \longmapsto & (t^2 + a_1 t - a_2, t^3 + a_1 t^2 - a_2 t) \end{array}$$

□

Corolário 3.1.3 *Seja E/K um curva elíptica com x e y suas funções coordenadas. Então*

$$K(E) = K(x, y) \text{ e } [K(E) : K(x)] = 2$$

□

À equação

$$Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6$$

chamamos de *equação de Weierstrass* da curva elíptica E/K, enquanto que as funções x, y são chamadas de *funções coordenadas da equação de Weierstrass*.

Este isomorfismo nos permite usar fórmulas explícitas para estudar várias propriedades de uma curva elíptica. Por exemplo, mais adiante veremos que a uma curva elíptica E/K podemos dar uma estrutura de grupo abeliano. No entanto, a estrutura deste grupo só poderá ser obtida mediante cálculos com sua equação de Weierstrass. É usando esta forma que se mostra um dos resultados mais celebrados sobre curva elíptica: o teorema de Mordell.

Entretanto, antes de tratarmos destes assuntos, façamos um estudo mais intenso da equação de Weierstrass.

3.2 Equação de Weierstrass

Na seção anterior vimos que associado a uma curva elíptica E/K existe uma equação de Weierstrass, no entanto para demonstrar este fato precisávamos escolher funções coordenadas de Weierstrass. Assim, podemos nos perguntar o quanto a equação de

Weierstrass depende de nossa escolha. O próximo resultado é uma resposta a esta pergunta...

Teorema 3.2.1 *Quaisquer duas equações de Weierstrass para uma curva elíptica E/K estão relacionadas por uma mudança linear de coordenadas do tipo:*

$$X = u^2X' + r$$

$$Y = u^3Y + suX' + t$$

com $u, r, s, t \in K$ e $u \neq 0$.

Prova: Sejam x, y e x', y' dois pares de funções coordenadas de Weierstrass para E. Então x, x' tem um pólo de ordem 2 em O e y, y' tem um pólo de ordem 3 em O. Além do mais $\{1, x\}$ e $\{1, x'\}$ são bases para $\mathcal{L}(2(O))$ e $\{1, x, y\}$ e $\{1, x', y'\}$ são bases para $\mathcal{L}(3(O))$.Efetuando uma mudança de base, podemos encontrar constantes $u_1, u_2, s_1, r, t \in K$, com $u_1, u_2 \neq 0$ de modo que:

$$x = u_1x' + r \qquad y = u_2y' + s_1x' + t$$

Entretanto $\{x, y\}$ e $\{x', y'\}$ satisfazem uma equação de Weierstrass nas quais os termos Y^2 e X^3 tem coeficiente 1, portanto $u_1^3 = u_2^2$. Colocando $u = u_2/u_1$ e $s = s_1/u^2$ temos a mudança de coordenadas desejada. □

Fazendo as substituições podemos computar os coeficientes a_i' para a nova equação

$$\begin{array}{rcl}
ua_1' & = & a_1 + 2s \\
u^2a_2' & = & a_2 - sa_1 + 3r - s^2 \\
u^3a_3' & = & a_3 + ra_1 + 2t = F_Y(r,t) \\
u^4a_4' & = & a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st = -F_X(r,t) - sF_Y(r,t) \\
u^6a_6' & = & a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - rta_1 - t^2 = -F(r,t)
\end{array}$$

Uma das razões para enumerarmos os coeficientes de uma equação de Weierstrass daquela maneira "aleatória" é que desta forma a relação entre os coeficientes antigos e os novos será obtida de uma forma mais "simétrica". Vejamos por exemplo o que acontece quando fazemos a trasformação $X = u^2X'$ e $Y = u^3Y'$. Neste caso a relação entre os coeficientes será dada de uma maneira muito simples, altamente

mnemônica: $a_i = u^i a'_i$.

Quando a característica de $K \neq 2$, podemos simplificar a equação de Weierstrass de uma curva elíptica, completando o quadrado em Y de

$$F(X,Y) = Y^2 + a_1XY + a_3Y - (X^3 + a_2X^2 + a_4X + a_6)$$

Para isso façamos a substituição $Y \to \frac{1}{2}(Y - a_1X - a_3)$:

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

$$(\frac{1}{2}(Y-a_1X-a_3))^2+a_1X(\frac{1}{2}(Y-a_1X-a_3))+a_3(\frac{1}{2}(Y-a_1X-a_3)) = X^3+a_2X^2+a_4X+a_6$$

$$(Y-a_1X-a_3)^2+2a_1X(Y-a_1X-a_3)+2a_3(Y-a_1X-a_3) = 4(X^3+a_2X^2+a_4X+a_6)$$

$$\begin{aligned} Y^2 + a_1X^2 + a_3^2 - 2a_1XY - 2a_3Y + 2a_1a_3X + 2a_1XY - 2a_1^2X^2 - 2a_1a_3X + \\ +2a_3Y - 2a_1a_3X - 2a_3^2 = 4X^3 + 4a_2X^2 + 4a_4X + 4a_6 \end{aligned}$$

$$Y^2 = 4X^3 + (4a_2 + a_1^2)X^2 + 2(2a_4 + a_1a_3)X + (4a_6 + a_3^2)$$

$$Y^2 = 4X^3 + b_2X^2 + 2b_4X + b_6 = g(X)$$

onde

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6 \end{aligned}$$

Se $\mathrm{char}(K) \neq 2, 3$ então fazendo as seguintes transformações $X \to \dfrac{(X - 3b_2)}{36}$ e $Y \to \dfrac{Y}{216}$ eliminamos o termo X^2 da equação simplificada, obtendo assim uma equação do tipo:

$$Y^2 = X^3 - 27c_4X - 54c_6 = f(X)$$

com $c_4 = b_2^2 - 24b_4$ e $c_6 = b_2^3 + 36b_2b_4 - 216b_6$.

Façamos, agora, o cálculo subseqüente:

$$\begin{aligned} d(Y^2 + a_1XY + a_3Y) &= d(X^3 + a_2X^2 + a_4X + a_6) \\ 2YdY + a_1YdX + a_1XdYa_3dY &= 3X^2dX + 2a_2XdX + a_4dX \\ (2Y + a_1X + a_3)dY &= (3X^2 + 2a_2X + a_4 - a_1Y)dX \\ \frac{dX}{2Y + a_1X + a_3} &= \frac{dY}{3X^2 + 2a_2X + a_4 - a_1Y} \\ \omega &= \frac{dY}{f_X(X,Y)} = \frac{dX}{f_Y(X,Y)} \end{aligned}$$

Chamamos a este diferencial ω de *diferencial invariante* da equação de Weierstrass.

Na seção anterior vimos a relação que uma curva elíptica tem com uma curva plana cúbica. Vimos também que se uma cúbica é não singular então ela será uma curva elíptica. No entanto, seria interessante saber se existe uma maneira mais efetiva de se mostrar que uma cúbica é não singular, por exemplo a partir dos seus coeficientes. Para isso definamos as seguintes quantidades associadas a uma equação de Weierstrass:

$$\begin{aligned} b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_3 + a_2a_3^2 - a_4^2 \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ j &= c_4^3/\Delta \end{aligned}$$

Verifica-se que estas quantidades satisfazem as seguintes relações :

$$4b_8 = b_2b_6 - b_4^2 \quad \text{e} \quad 1728\Delta = c_4^3 - c_6^2$$

Chamamos Δ de *discriminante* associado a equação de Weierstrass, enquanto que j é chamado de *j-invariante* da curva elíptica E.

A tabela abaixo resume o que acontece com os coeficientes quando fazemos mudanças de variáveis que preservam a equação de Weierstrass, isto é:

$$X = u^2X' + r$$

$$Y = u^3Y + suX' + t$$

$$
\begin{array}{rcl}
u^2 b_2' & = & b_2 + 12r = 1/2g''(r) \\
u^4 b_4' & = & b_4 + b_2 r + 6r^2 = 1/2g'(r) \\
u^6 b_6' & = & b_6 + 2b_4 r + b_2 r^2 + 4r^3 = g(r) \\
u^8 b_8' & = & b_8 + 3b_6 r + 3r^2 b_4 + b_2 r^3 + 3r^4 \\
u^4 c_4' & = & c_4 \\
u^6 c_6' & = & c_6 \\
u^{12}\Delta' & = & \Delta \\
j' & = & j \\
u^{-1}\omega' & = & \omega
\end{array}
$$

onde $g'(X)$ e $g''(X)$ representa, respectivamente, a primeira e a segunda derivada do o polinômio obtido a partir da mudança que deixa a equação de Weierstrass com a forma $Y^2 = g(X) = 4X^3 + b_2X^2 + 2b_4X + b_6$.

Observe que o j-invariante não tem este nome por acaso: afinal ele é um invariante da classe de isomorfismo da curva, independendo da equação de Weierstrass escolhida para E.

Enfim consideremos uma curva E em $\mathbb{P}^2_K$ definida por uma equação de Weierstrass.

Teorema 3.2.2 *E é não singular se, e somente se, $\Delta \neq 0$*
Prova: Mostramos que para um corpo de característica $\neq 2$ a equação de Weierstrass assume a seguinte forma:

$$F(X, Y) = Y^2 - g(X)$$

com $g(X)$ um polinômio de grau 3. Então para que um ponto desta curva E seja singular deveremos ter

$$
\begin{array}{rcl}
\dfrac{\partial F}{\partial Y}(x_0, y_0) & = & 2y_0 = 0 \\
\dfrac{\partial F}{\partial X}(x_0, y_0) & = & g'(x_0) = 0
\end{array}
$$

Assim um ponto em E será singular se, e somente se, for da forma $(0, x_0)$ com x_0 uma raiz dupla do polinômio $g(X)$. Entretanto para sabermos se g possui uma

raíz dupla basta mostrarmos que $\mathrm{Disc}(g) = \mathrm{Res}(g, g') = 0$. É só uma questão de cálculos mostrar que Δ e $\mathrm{Disc}(g)$ são iguais módulo uma constante não nula.

Caso $\mathrm{char}(K) = 2$ teremos que:

$$\begin{aligned} b_2 &= a_1^2 \\ c_4 &= b_2^2 = a_1^4 \\ j &= c_4^3/\Delta = a_1^{12}/\Delta \end{aligned}$$

Em particular $a_1 = 0$ se, e só se, $j = 0$.

Suponhamos que $j \neq 0$ ou equivalentemente que $a_1 \neq 0$. Substituindo X por $X + c$ teremos que $Y^2 + a_1XY + a_3$ se transforma em $Y^2 + a_1XY + (a_1c + a_3)Y$. Logo tomando $c = -a_3/a_1$ podemos supor que $a_3 = 0$ e que o primeiro membro da equação de Weierstrass é da forma $Y^2 + a_1XY$. Substituindo X por a_1^3X e Y por a_1^3Y permite-nos normalizar $a_1 = 1$ e uma mudança de variáveis linear permite-no escolher $a_4 = 0$. Enfim:

$$Y^2 + XY = X^3 + a_2X^2 + a_6$$

Desta forma teremos $b_2 = 1$, $b_4 = b_6 = 0$, $b_8 = a_6$, e $c_4 = 1$ e $\Delta = a_6 = 1/j$. As derivadas parciais para esta equação de Weierstrass são:

$$\begin{aligned} F_X &= Y + X^2 \\ F_Y &= X \end{aligned}$$

Logo o ponto singular será a origem $(0, 0)$. No entanto, este ponto pertence a curva se, e somente se, $a_6 = \Delta = 0$. Portanto E é lisa se, e somente se, $\Delta \neq 0$.

No caso de termos $j = 0$, significando assim que $a_1 = 0$, a equação de Weierstrass para esta curva será

$$Y^2 + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

e teremos para esta equação $b_2 = b_4 = 0$, $b_8 = a_4^2$ e $\Delta = a_3^4$. As derivadas parciais são

$$\begin{aligned} F_X &= X^2 + a_4 \\ F_Y &= a_3 \end{aligned}$$

Ficando claro que se a curva for singular então $\Delta = a_3^4 = 0$. Caso $\Delta = a_3^4 = f_Y = 0$ então a curva é dada por

$$Y^2 = X^3 + a_2X^2 + a_4X + a_6$$

Fazendo a substituição $X \to X + a_2$ e $Y \to Y$ obtemos

$$Y^2 = X^3 + a_4X + a_6 = h(X)$$

Como Δ é o discriminante de $h(X)$, a menos de uma constante, teremos que a curva será singular uma vez que $f_X = h'(X) = 0$. □

Vimos anteriormente que duas curvas elípticas isomorfas possuem o mesmo j-invariante. Na realidade, vale também a recíproca desta afirmação: *Se duas curva elíptica E/K e E'/K possuem o mesmo j-invariante então elas são isomorfas sobre* $\bar{K}$. A demonstração deste fato para característica 2 e 3 requer algumas considerações que não faremos aqui. Façamos apenas o caso mais simples: $\text{char}(K) \neq 2, 3$.

Como vimos as equações das curvas elípticas E/K e E'/K podem ser dadas por $Y^2 = X^3 + aX + b$ e $Y'^2 = X'^3 + a'X' + b'$, respectivamente. Para esta curvas os j-invariantes são

$$j(E) = \frac{4a^3}{4a^3 + 27b^2} = \frac{4a'^3}{4a'^3 + 27b'^2} = j(E')$$

donde

$$\begin{aligned} (4a)^3(4a'^3 + 27b'^2) &= (4a')^3(4a^3 + 27b^2) \\ 4^4(aa')^3 + 4.27a^3b'^2 &= 4^4(aa')^3 + 4.27a'^3b^2 \\ a^3b'^2 &= a'^3b^2 \end{aligned}$$

Se $a = 0$ então $b \neq 0$, pois $\Delta \neq 0$, e daí $a' = 0$ o que nos leva a concluir que $b' \neq 0$. Portanto $X \to (b/b')^{\frac{1}{3}}X'$ e $Y \to (b/b')^{\frac{1}{2}}Y'$ será um isomorfismo.

$b = 0 \Rightarrow a \neq 0 \Rightarrow a' \neq 0$. Portanto as transformações $X \to (a/a')^{\frac{1}{2}}X'$ e $Y \to (a/a')^{\frac{3}{4}}Y'$ nos dão um isomorfismo.

Já se $ab \neq 0$, uma vez que $a' = 0 \Rightarrow b' = 0$ contradizendo $\Delta' \neq 0$, teremos que $a'b' \neq 0$ então tomando quaisquer uma das transformações acima teremos o isomorfismo desejado.

Seja $j_0 \in \bar{K}$. Se $j_0 \neq 0, 1728$, então a curva

$$E : Y^2 + XY = X^3 - \frac{36}{j_0 - 1728}X - \frac{1}{j_0 - 1728}$$

tem j_0 como j-invariante e seu discriminante é $\Delta = \frac{j_0^2}{(j_0 - 1728)^3}$. Note que E está definida sobre $K(j_0)$.

Para $j_0 = 0$ temos a curva

$$E : Y^2 + Y = X^3 \qquad \Delta = -27$$

Enquanto que para $j_0 = 1728$ a curva

$$E : Y^2 = X^3 + X \qquad \Delta = -64$$

terá j-invariante igual a 1728. Observe que em caracaterística 2 ou 3, $j_0 = 1728 = 12^3 = 0$, mas ainda assim um dos exemplos servirá.

3.3 Lei de Grupo

Para curvas lisas de gênero 0 sobre os racionais vimos que a existência de um ponto racional faz com que esta curva seja isomorfa sobre $\mathbb{Q}$ a uma reta. Também vimos que o princípio local-global é uma maneira de determinar quando uma curva de gênero 0 possui ou não um ponto racional. Logo, pode-se determinar totalmente a estrutura dos pontos racionais de uma curva com gênero 0.

Entretanto para curvas de gênero 1 não existe ainda tal ferramenta: não se pode dizer que uma curva de gênero 1 possui um ponto racional apenas analisando o que acontece localmente. Um contra-exemplo para este princípio é a curva que Selmer mostrou ter pontos em $\mathbb{Q}_p, \forall p \geq 2$ primo mas que não possui nenhum ponto racional: $3X^3 + 4Y^3 + 5Z^3 = 0$.

Por isso que, para o estudo de curvas $\mathcal{C}$ de gênero 1, a condição de existência de um ponto racional é primordial, sem esta condição quase nada se pode dizer a respeito da curva. A existência de um ponto racional, como mostraremos aqui, fará com que $\mathcal{C}(K)$ tenha uma estrutura de grupo.

Inicialmente, vejamos o que acontece com uma cúbica cujo ponto K-racional (ponto com coordenadas em K) O é singular. Como O é singular cada reta K-racional (i.e., reta definida sobre K) intercepta a curva em um outro ponto P que também será racional pois sua coordenada x, por exemplo, será solução de uma equação cúbica que já possui duas outras soluções K-racionais referentes ao ponto O. Desta forma, a reta que une O a P é uma reta definida sobre K e interceptará uma outra reta definida sobre K em um ponto K-racional. Em outras palavras, podemos projetar a cúbica numa reta definida sobre K através do ponto O, de modo que a pontos K-racionais da reta estejam em bijeção com os pontos K-racionais da cúbica.

Já para cúbicas lisas teremos que, dado um ponto K-racional, qualquer reta passando por este ponto interceptará a curva em dois outros pontos (distintos ou não). Assim não poderíamos de uma maneira geral fazer uma correspondência biunívoca entre os pontos K-racionais desta cúbica e os pontos da reta.

Contudo, se tivermos dois pontos K-racionais P e Q, a reta que os une estará definida sobre K e cortará a cúbica num ponto PQ, que deverá ser K-racional (para isso basta notarmos que a equação que permite calcular esta interseção será de grau três e possurá duas raízes em K correspondentes aos pontos P e Q). Obtemos, então, um tipo de operação para dois pontos K-racionais distintos desta curva.

Para estendermos esta operação façamos associar ao ponto P um outro ponto K-racional PP obtido através da interseção da cúbica com a reta tangente em P. Logo de poucos pontos K-racionais sobre a curva podemos possivelmente obter infinitos outros. A este método de obtenção de pontos K-racionais a partir de outros chamaremos de *corda-tangente*.

Esta operação, entretanto, apesar de ser comutativa, não possui ao menos um elemento neutro que seria um ponto 0 tal que todas as retas tangentes a um ponto P desta cúbica passe por 0. Entretanto fazendo alguns aperfeiçoamentos nesta operação obtém-se uma lei de grupo para uma cúbica não singular. Para isto, necessitaremos do ponto K-racional P da cúbica.

Como vimos esta cúbica é uma curva elíptica isomorfa a uma cúbica E dada por uma equação de Weierstrass. O ponto P é então levado no ponto $O = (0 : 1 : 0)$.

Este ponto O será o elemento neutro do grupo dado pela operação:

Definição 3.2 *Dados P e Q na curva, obtemos pelo método corda-tangente o ponto PQ. Seja L' a reta ligando PQ a O. L' intercepta E num outro ponto que denotaremos por $P + Q$.*

Em símbolos temos $P + Q = O(PQ)$.

Lema 3.3.1 *Sejam $\mathcal{C}$ uma curva de gênero 1 e $P, Q \in \mathcal{C}$. Então $(P) \sim (Q)$ se, e somente se, $P = Q$.*
Prova: Se $(P) \sim (Q)$ então existe $f \in \bar{K}(C)$ tal que $(P) - (Q) = \text{div}(f) \Rightarrow \text{div}(f) + (Q) = (P) \geq 0$. Logo $f \in \mathcal{L}((Q))$. Pelo Riemann-Roch (**1.5.4**, pg. 22), $\ell((Q)) = 1$, logo $f \in \mathcal{L}((Q)) = \bar{K}$ e $(P) - (Q) = \text{div}(f) = 0$, ou seja, $P = Q$. □

Lema 3.3.2 *Seja $\mathcal{C}$ uma curva cúbica não singular e $\mathcal{C}_1$ e $\mathcal{C}_2$ duas outras curvas cúbicas distintas. Se oito dos pontos da interseção entre $\mathcal{C}_1$ e $\mathcal{C}$ estão na interseção de $\mathcal{C}_2$ e $\mathcal{C}$ então $\mathcal{C}_1$ e $\mathcal{C}_2$ interceptam $\mathcal{C}$ nos mesmos nove pontos.*
Prova: Sejam f_1 e f_2 os polinômios que definem $\mathcal{C}_1$ e $\mathcal{C}_2$, respectivamente. Claramente temos que $\dfrac{f_1}{f_2} \in K(\mathcal{C})$ e:

$$\text{div}(\frac{f_1}{f_2}) = \sum_{i=1}^{8}(P_i) + (Q) - (\sum_{i=1}^{8}(P_i) + (P)) = (Q) - (P)$$

Em outras palavras, $(Q) \sim (P)$. Como toda cúbica lisa tem gênero 1, pelo lema anterior tem-se que $Q = P$. □

Teorema 3.3.3 *A operacão definida acima é uma lei de grupo para E cujo elemento neutro é O. Ademais E é grupo abeliano e esta lei de grupo satisfaz:*
$(*)$ *$P + Q + R = O$ se, e só se, P, Q e R estiverem numa mesma reta.*
Prova: A propriedade $(*)$ mostra-se notando que se P, Q e R estão sobre uma mesma reta então $PQ = R$. Daí teremos que $P + Q = OR$. A reta unindo OR a R intercepta a curva no ponto O, o que mostra que $(P + Q)R = O$. Como O é um ponto de tangente inflexional teremos exatamente que $(P + Q) + R = O$. No entanto, mostraremos, logo a seguir, que $+$ é uma operação de grupo, valendo assim $P + Q + R = O$.

Para que E/K seja um grupo abeliano deve-se mostrar que $\forall P, Q, R \in E(K)$ valem :

- $P + Q = Q + P$

  $P+Q = O(PQ) = O(QP) = Q+P$ uma vez que a operação PQ é comutativa.

- $P + O = P$

  A reta que une PO a O claramente intercepta E em P, donde obtemos o resultado.

- $\exists - P \in E$ tal que $P + (-P) = O$

  PO, P e O estão sobre a mesma reta. Portanto por $(*)$ temos que $(PO+O)+P = O$. Usando, o item anterior temos que $PO+P = 0$. Tomamos então $-P = OP$.

- $(P + Q) + R = P + (Q + R)$

  Para a associatividade basta mostrarmos que $(P + Q)R = P(Q + R)$ pois assim a reta que une O a este ponto daria o mesmo ponto que por um lado é $(P + Q) + R$ e por outro lado é $P + (Q + R)$.

  Sejam l a reta que passa por P,Q e PQ; m a reta que passa por $P + Q$, R e $(P+Q)R$; e n a reta que passa por O, QR e $Q+R$. Então a cúbica $l \cdot m \cdot n = 0$ intercepta E em $O, P, Q, R, PQ, QR, P + Q, Q + R$ e $(P + Q)R$.

  Consideremos a reta r que passa por P, $Q + R$ e $P(Q + R)$; a reta s que une os pontos Q, R e QR; e a reta t passando por O, PQ e $P + Q$. Portanto a cúbica $r.s.t = 0$ intercepta E nos pontos $O, P, Q, R, PQ, QR, P + Q, Q + R$ e $P(Q + R)$.

  Pelo lema anterior, vemos que $P(Q + R) = (P + Q)R$. Logo a operação é associativa.

□

Assim vemos que dada uma curva cúbica lisa podemos dotá-la de uma estrutura de grupo definida geometricamente. Todavia, também a partir da definição de curva elíptica podemos torná-la um grupo da seguinte forma

Teorema 3.3.4 *Seja (E, O) uma curva elíptica.*
(a) Existe uma bijeção de conjuntos $\sigma : \mathrm{Pic}^0(E) \to E$.
(b) Se E é dada por uma equação de Weierstrass, então a "lei de grupo geométrica" em E e a "lei de grupo algébrica" induzida por $\mathrm{Pic}^0(E)$ são as mesmas.

Prova: (a) Como E tem gênero 1, pelo Riemmann-Roch (**1.5.4**, pg. 22), temos que

$$\dim_{\bar{K}} \mathcal{L}(D + (O)) = \deg(D + (O)) = 1$$

Seja $f \in \bar{K}(E)$ um gerador para $\mathcal{L}(D + (O))$. Temos que

$$\operatorname{div}(f) \geq -D - (O) \qquad \text{e} \qquad \deg(\operatorname{div}(f)) = 0$$

e daí existirá um $Q \in E$ tal que

$$\operatorname{div}(f) = -D - (O) + (Q) \Longrightarrow D \sim (Q) - (O)$$

Além disso Q é único pois, para qualquer outro Q' que satisfaça isto teremos

$$(Q) - (O) \sim D \sim (Q') - (O) \Longleftrightarrow (Q) \sim D + (O) \sim (Q')$$

Uma vez mais, usando um dos lemas anteriores, teremos que $Q = Q'$.

Esta propriedade define uma função:

$$\gamma : \operatorname{Div}^0(E) \to E$$

sobrejetiva, já que para todo $P \in E$ temos

$$(P) - (O) \sim (P) - (O)$$

isto é,

$$\gamma((P) - (O)) = P$$

Consideremos a função:

$$\begin{array}{rccc} \sigma : \operatorname{Pic}^0(E) & \longrightarrow & E \\ \tilde{D} & \longmapsto & \gamma(D) \end{array}$$

onde denotamos por $\tilde{D}$ a classe de $D \in \operatorname{Div}^0(E)$ em $\operatorname{Pic}^0(E)$.

Este mapa é claramente sobrejetivo. Se para $D_1, D_2 \in \operatorname{Div}^0(E)$ com $\gamma(D_i) = P_i$ tivermos $\sigma(\tilde{D_1}) = P_1 = P_2 = \sigma(\tilde{D_2})$ então

$$D_1 \sim (P_1) - (O) = (P_2) - (0) \sim D_2$$

Ou seja, σ é injetiva.

(b) Seja então E dada por uma equação de Weierstrass e $P, Q \in E$. É suficiente mostrarmos que

$$\sigma^{-1}(P+Q) = \sigma^{-1}(P) + \sigma^{-1}(Q)$$

Claramente $\sigma^{-1} : E \to \mathrm{Pic}^0(E)$ é dada por $\sigma^{-1}(P) = \widetilde{(P) - (O)}$.

Consideremos a reta L, dada pelo polinômio f, que passa por P, Q e PQ. Consideremos, também a reta L', dada pelo polinômio f', passando por O, PQ e $P+Q$. Claramente $f/Z, f'/Z \in \bar{K}(E)$ e temos:

O fato da reta $Z = 0$ interceptar E em O com multiplicidade 3 garante que

$$\begin{aligned} \mathrm{div}(f/Z) &= (P) + (Q) + (PQ) - 3(O) \\ \mathrm{div}(f'/Z) &= (O) + (PQ) + (P+Q) - 3(O) = (PQ) + (P+Q) - 2(O) \end{aligned}$$

Então

$$\begin{aligned} \mathrm{div}(\frac{f'}{f}) &= \mathrm{div}(f'/Z) - \mathrm{div}(f/Z) \\ &= (O) + (PQ) + (P+Q) - 2(O) - (P) - (Q) - (PQ) + 3(O) \\ &= (P+Q) - (P) - (Q) + (O) \end{aligned}$$

Logo temos que

$$\begin{aligned} (P+Q) &\sim (P) + (Q) - (O) \\ (P+Q) - (O) &\sim (P) - (O) + (Q) - (O) \\ \widetilde{(P+Q)} &= \widetilde{(P)} + \widetilde{(Q)} \\ \sigma^{-1}(P+Q) &= \sigma^{-1}(P) + \sigma^{-1}(Q). \end{aligned}$$

□

Para $m \in \mathbb{Z}$ e $P \in E$ denotaremos

$$\begin{cases} [0]P = O \\ [m]P = [m-1]P + P & \text{se } m > 0 \\ [m]P = [-m](-P) & \text{se } m < 0 \end{cases}$$

Corolário 3.3.5 *Seja E uma curva elíptica e $D = \sum n_P(P) \in \mathrm{Div}(E)$. Então são equivalentes:*
(i) D é principal;
(ii) $\sum n_P = 0$ e $\sum [n_P]P = O$.
Prova: Suponhamos que $\sum n_P = 0$ já que D principal implica $D \in \mathrm{Div}^0(E)$. Logo usando o isomorfismo $\sigma^{-1} : E \to \mathrm{Pic}^0(E)$ temos

$$\begin{aligned}
\sigma^{-1}(\sum [n_P]P) &= \sum n_P \sigma^{-1}(P) \\
&= \sum n_P \widetilde{(P) - (O)} \\
&= \sum n_P \widetilde{(P)} - \sum n_P(O) \\
&= \widetilde{\sum n_P(P)} (\text{ já que } \sum n_P = 0) \\
&= \widetilde{D}
\end{aligned}$$

Logo D é principal se, e somente se, $\tilde{D} = 0 = \sigma^{-1}(O)$ se, e somente se, $\sum [n_P]P = O$. □

Agora, a partir da equação de Weierstrass derivaremos fórmulas explícitas para a lei de grupo numa curva elíptica. Estas fórmulas, dentre outras coisas, permitirão mostrar que a soma de dois pontos $+ : E \times E \to E$ é um morfismo, além de dar uma maneira efetiva de calcular soluções racionais de uma cúbica lisa a partir de outras.

Seja $E(K)$ uma curva elíptica com a equação de Weierstrass

$$F(X, Y) = Y^3 + a_1XY + a_2Y - X^3 - a_2X^2 - a_4X - a_6 = 0$$

e seja $P = (x_0, y_0) \in E$. Vejamos como calcular $-P$.

Na demonstração geométrica da lei de grupo, vimos que $-P$ é o terceiro ponto de interseção da reta ligando O a P. A reta ligando O a P tem equação $X = x_0$ e para acharmos sua terceira interseção com E basta substituirmos x por x_0 na equação de Weierstrass

$$Y^2 + (a_1x_0 + a_2)Y - x_0^3 - a_2x_0^2 - a_4x_0 - a_6 = 0$$

A outra solução y_0' desta equação quadrática em Y será a segunda coordenada do ponto $-P$. Daí

$$F(x_0, Y) = (Y - y_0)(Y - y_0') = Y^2 - (y_0 + y_0')Y + y_0y_0'$$

Comparando os coeficientes obtemos a relação

$$-(y_0 + y_0') = a_1x_0 + a_2 \Longrightarrow y_0' = -y_0 - a_1x_0 - a_2$$

Donde

$$-P = (x_0, -y_0 - a_1x_0 - a_2)$$

Consideremos dois pontos de E, $P_1 = (x_1, x_2)$ e $P_2 = (x_2, y_2)$, e vejamos como encontrar uma fórmula para a soma destes pontos.

Se $x_1 = x_2$ e $y_2 = -y_1 + a_1x_0 + a_2$ então pelos cálculos que acabamos de fazer temos que $P_1 + P_2 = O$. Caso contrário a reta L unindo P_1 a P_2 terá equação da forma

$$L : Y = \lambda X + v$$

onde λ e v são dados pelas fórmulas:

- Caso $x_1 = x_2$
  Então

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$$

e

$$v = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$$

  Pois, neste caso, a reta L será a reta tangente a E em P_1. A equação dessa reta tangente é dada por

$$y - y_1 = \frac{dY}{dX}(P)(x - x_1)$$

  Derivando implicitamente $Y^3 + a_1XY + a_2Y - X^3 - a_2X^2 - a_4X - a_6$ em relação a X temos:

$$2Y\frac{dY}{dX} + a_1X\frac{dY}{dX} + a_1Y + a_3\frac{dY}{dX} = 3X^2 + 2a_2X + a_4$$

  Depois de avaliar $\dfrac{dY}{dX}$ no ponto P_1, substituímos este resultado na equação da reta tangente e alguns cálculos a mais nos dão o resultado desejado.

- Caso $x_1 \neq x_2$
  Então
  $$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$
  e
  $$v = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$$
  Pois neste caso, a reta que passa por P_1 e P_2 tem exatamente inclinação λ dada acima.

Ao substituirmos a equação de L na equação de E veremos que o polinômio em X, $F(X, \lambda X + v)$, terá três soluções x_1, x_2, x_3; onde $P_3 = (x_3, y_3)$ é o terceiro ponto de interseção de E e L. Um mero cálculo mostra que o coeficiente do termo de 2^o grau em $F(X, \lambda X + v)$ é

$$\lambda^2 + a_1\lambda - a_2$$

Como $F(X, \lambda X + v) = (X - x_1)(X - x_2)(X - x_3)$ vemos que:

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$$

Para obter a coordenada y_3 basta lembrarmos que P_3 também pertence a reta L, donde

$$y_3 = \lambda x_3 + v$$

Como P_1, P_2 e P_3 pertencem a mesma reta teremos

$$P_1 + P_2 + P_3 = O \Longrightarrow P_1 + P_2 = -P_3$$

Aplicando a fórmula da inversão obtemos

$$P_1 + P_2 = (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, -(x_3 + a_1)\lambda - v - a_3)$$

Estas fórmulas serão necessárias quando formos demonstrar o Teorema de Mordell. No entanto, a demonstração dada aqui para este belíssimo teorema será feita para curvas elípticas sobre $\mathbb{Q}$, o que nos permite simplificar bastante as fórmulas encontradas:

Corolário 3.3.6 *Seja $E = E(\mathbb{Q})$ dada por*

$$Y^2 = X^3 + aX + b$$

Sejam $P = (x, y)$, $P_1 = (x_1, x_2)$ e $P_2 = (x_2, y_x)$ pontos de E. Então:
(a) $-P = (x, -y)$
(b) Se $x_1 \neq x_2$ então

$$\begin{aligned} x(P_1 + P_2) &= (\frac{y_2 - y_1}{x_2 - x_1})^2 - (x_1 + x_2) \\ y(P_1 + P_2) &= -(\frac{y_2 - y_1}{x_2 - x_1})^3 + \frac{y_2 - y_1}{x_2 - x_1}(x_1 + x_2) - \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1} \end{aligned}$$

(c) A fórmula da duplicação:

$$\begin{aligned} x([2]P) &= \frac{(3x^2 + a)^2 - 8x(x^3 + ax + b)}{4(x^3 + ax + b)} = \frac{x^4 - 2ax^2 - 8bx + a^2}{4y^2} \\ y([2]P) &= \frac{(3x^2 + a)^3 + 4(x^3 + ax + b)(7x^3 + ax - 2b)}{8(x^3 + ax + b)^3} \end{aligned}$$

3.4 Isogenias

Quando se estuda algum tipo de estrutura, anéis, corpos, módulos, grupos, etc., as aplicações entre elas possuem um papel de grande importância, pois revelam semelhanças e propriedades ocultas que de outra maneira jamais poderíamos suspeitar. Para tanto estas aplicações deverão preservar as principais características da estrutura; é por isso que os homomorfismos entre grupos preservam a operação do grupo, ou as aplicações contínuas entre espaços topológicos são definidas a partir de abertos.

Como as curvas elípticas, além de serem variedades, são também grupos, uma aplicação "interessante" entre curvas elípticas deve ser um morfismo de curvas e um homomorfismo de grupos. Todavia, como veremos adiante, não é necessário se exigir tanto.

Definição 3.3 *Seja $\phi : E_1 \to E_2$ um mapa entre curvas elípticas $< E_1, O_1 >$ e $< E_2, O_2 >$ definidas sobre k. ϕ é uma* isogenia *se ϕ é um morfismo entre curvas*

tal que $\phi(O_1) = O_2$. *Diremos que duas curvas elípticas são* isógenas *quando existir uma isogenia não constante entre elas, isto é,* $\phi(E_1) \neq O_2$

Como todo morfismo entre curvas é constante ou sobrejetivo (**1.2.4**, pg. 13) teremos que uma isogenia ϕ satisfaz $\phi(E_1) = O_2$ ou $\phi(E_1) = E_2$, donde toda isogenia, exceto a isogenia $[0]P = O_2$, é um mapa finito entre curvas. Conseqüentemente, existirá uma injeção entre os corpos de funções

$$\phi^* : \bar{k}(E_2) \to \bar{k}(E_1)$$

e o grau de ϕ ($\deg \phi$), o grau separável de ϕ ($\deg_s \phi$), o grau inseparável de ϕ ($\deg_i \phi$), a separabilidade de ϕ, a inseparabilidade de ϕ ou se ϕ é puramente inseparável são definidos pela propriedade correspondente para a extensão finita $\bar{k}(E_2)/\phi^*(\bar{k}(E_1))$. Convenciona-se: $\deg[0] = 0$.

A nossa definição de isogenias, ao contrário do que poderia ser, não menciona nada sobre grupos; também não é necessário:

Proposição 3.4.1 *Toda isogenia* $\phi : E_1 \to E_2$ *é um homomorfismo de grupos.*
Prova: Devemos mostrar que

$$\phi(P + Q) = \phi(P) + \phi(Q)$$

para todos os pontos $P, Q \in E_1$.

Para a isogenia constante [0] nada há para demonstrar. Caso ϕ seja um mapa finito, ele induzirá um homomorfismo

$$\phi_* : \mathrm{Pic}^0(E_1) \to \mathrm{Pic}^0(E_2)$$

definido por

$$\phi_*(\overline{\sum_i n_i(P_i)}) = \sum_i n_i \overline{\phi(P_i)}$$

Por outro lado existem isomorfismos de grupos

$$\begin{array}{ccc} \kappa_i : E_i & \longrightarrow & \mathrm{Pic}^0(E_i) \\ P & \longmapsto & \overline{(P) - (O_i)} \end{array}$$

Donde, $\forall P \in E_1$, temos

$$\begin{aligned}
\kappa_2 \circ \phi(P) &= \kappa_2(\phi(P)) = \overline{(\phi(P)) - (O_2)} \\
&= \overline{(\phi(P)) - (\phi(O_1))} \\
&= \phi_*((P) - (O_1)) \\
&= \phi_*(\kappa_1(P)) \\
&= \phi_* \circ \kappa_1(P)
\end{aligned}$$

ou seja

$$\kappa_2 \circ \phi = \phi_* \circ \kappa_1$$

Consideremos P e Q pontos quaisquer de E_1. Logo, como κ_1, κ_2 e ϕ_* são homomorfismos

$$\begin{aligned}
\kappa_2(\phi(P+Q)) &= \kappa_2 \circ \phi(P+Q) \\
&= \phi_* \circ \kappa_1(P+Q) \\
&= \phi_*(\kappa_1(P) + \kappa_1(Q)) \\
&= \phi_* \circ \kappa_1(P) + \phi_* \circ \kappa_1(Q) \\
&= \kappa_2 \circ \phi(P) + \kappa_2 \circ \phi(Q) \\
&= \kappa_2(\phi(P) + \phi(Q))
\end{aligned}$$

O resultado segue desta igualdade, pois κ_2 é injetivo. □

Uma pergunta natural surge: $\mathrm{Hom}(E_1, E_2) = \{\phi : E_1 \to E_2 \mid \phi \text{ é uma isogenia}\}$ possui algum tipo de estrutura? Se soubessémos que a adição de pontos é um morfismo, poderíamos dotá-lo de uma estrutura de grupo com a seguinte lei de adição:

$$(\phi + \psi)(P) = \phi(P) + \psi(P)$$

O resultado abaixo é a garantia deste fato:

Teorema 3.4.1 *Seja E/K uma curva elíptica. Então as fórmulas que dão a lei de adição em E definem morfismos*

$$\begin{array}{ccc} + : E \times E & \longrightarrow & E \\ (P_1, P_2) & \longmapsto & P_1 + P_2 \end{array} \quad e \quad \begin{array}{ccc} - : E & \longrightarrow & E \\ P & \longmapsto & -P \end{array}$$

Prova: O mapa

$$\begin{array}{rcl} - : E & \longrightarrow & E \\ (x,y) & \longmapsto & -(x,y) = (x, -y - a_1x - a_3) \end{array}$$

é claramente racional. Como E é lisa, então $-$ é um morfismo.

Pelas fórmulas de adição de pontos descritas na seção anterior (**3.3**, pg. 67), vemos que o mapa $+ : E \times E \to E$ é um morfismo no ponto (P, Q) quando $P \neq O$ ou $Q \neq O$, ou quando $x_1 \neq x_2$, $P = (x_1, y_1)$ e $Q = (x_2, y_2)$. Como $x_1 = x_2$ implica que $y_2 = y_1$ ou $y_2 = -y_1 - a_1x_2 - a_3$ então o último caso equivale a dizer que $P \neq Q$ ou $P \neq -Q$.

Consideremos, para um ponto $R \in E$, o mapa s_R que associa a um ponto $Q \neq P$ o terceiro ponto da interseção de E com a reta que une R a Q. Obviamente $s_R(Q) = -(R + Q)$ e as fórmulas da seção anterior nos dizem que, para $R = (x_1 : y_1 : 1)$ e $Q = (x_2 : y_2 : 1)$, temos

$$\begin{array}{rl} s_R(Q) & = \\ & ((y_2 - y_1)^2 + a_1(y_2 - y_1)(x_2 - x_1) + (-a_2 - x_1 - x_2)(x_2 - x_1)^2 : \\ & : (y_2 - y_1 + y_1x_2 - y_2x_1)(x_2 - x_1) : (x_2 - x_1)^2) \end{array}$$

um mapa regular se $R \neq Q$. Usando a equação de Weierstrass da curva elíptica conseguimos mostrar que s_R também é regular em R, logo s_R é um morfismo (**1.2.1**, pg. 12). Mais ainda, s_R é um automorfismo pois $(s_R)^2 = \mathrm{Id}$. Mostremos agora que $s_R(R)$ é exatamente o terceiro ponto da interceção da tangente em R com E.

Dentro da demonstração do isomorfismo (**3.3.4**, pg. 62) $\sigma^{-1} : E \to \mathrm{Pic}^0(E)$ chegamos as seguintes relações com divisores:

$$(R) + (P) + (Q) \sim 3(O) \Longleftrightarrow R, P \text{ e } Q \text{ estão alinhados} \tag{3.1}$$

$$(P) + (Q) \sim (R) + (O) \Longleftrightarrow P + Q = R \tag{3.2}$$

A partir da definição da função s_R, a relação (3.1) lê-se

$$(Q) + (R) + (s_R(Q)) \sim 3(O)$$

Como s_R é um automorfismo, a aplicação

$$\begin{array}{rcl} (s_R)_* : \mathrm{Div}(E) & \longrightarrow & \mathrm{Div}(E) \\ (P) & \longmapsto & (s_R(P)) \end{array}$$

(conforme (**1.3**, pg. 18)) preserva equivalência linear entre divisores e portanto

$$\begin{aligned}(s_R(Q)) + (s_R(R)) + (s_R(s_R(Q))) &\sim 3(s_R(O)) \\ (-R-Q) + (s_R(R)) + (Q) &\sim 3(-R)\end{aligned}$$

já que $s_R(O) = -R$. De (7.1) obtemos as relações

$$\begin{aligned}(-Q-R) &\sim (-R) + (-Q) - (O) \\ (-Q) + (Q) &\sim 2(O)\end{aligned}$$

e daí

$$\begin{aligned}(-R-Q) + (s_R(R)) + (Q) &\sim 3(-R) \\ (-R) + (-Q) - (O) + (s_R(R)) + (Q) &\sim 3(-R) \\ (s_R(R)) + (Q) + (-Q) - (O) &\sim 2(-R) \\ (s_R(R)) + (O) &\sim (-R) + (-R)\end{aligned}$$

e a relação (7.1) nos diz que

$$s_R(R) = [2](-R)$$

isto é, $[-2]R$ é o terceiro ponto da interseção de E com a reta tangente em R.

Consideremos o mapa $\tau_R(Q) = R + Q$. Pela definição de s_R e a definição geométrica da soma de dois pontos temos que $\tau_R = s_O \circ s_R$, e daí temos que portanto τ_Q é um automorfismo, para qualquer $Q \in E$, com inversa τ_{-Q}. Finalmente, para qualquer $P, Q \in E$ temos

$$\tau_{R+S} \circ +(P, Q) = +(\tau_R(P), \tau_S(Q))$$

Portanto se $+$ é um morfismo no ponto (P, Q) então ela também será um morfismo no ponto $(\tau_R(P), \tau_S(Q))$.

Suponha $P \neq O$ e considere os casos abaixo.

Se $T \neq O$, então $+$ é um morfismo em $(P, P - T)$ uma vez que $P \neq P - T$ e daí será um morfismo também em

$$(\tau_O(P), \tau_T(P - T)) = (P, P)$$

Se $-T \neq P$ então $+$ é um morfismo em $(P, -T)$ e daí será um morfismo em

$$(\tau_O(P), \tau_{T-P}(-T)) = (P, -P)$$

$+$ será um morfismo em (P,T) e (T,P) se $P \neq T$ então será também um morfismo em

$$(\tau_O(P), \tau_{-T}(T)) = (P,O), \quad (\tau_{-T}(T), \tau_O(P)) = (O,P) \quad \text{e} \quad (\tau_{-P}(P), \tau_{-T}(T)) = (O,O)$$

□

Quando $E_1 = E_2$, então podemos ainda compor isogenias. Portanto para uma curva elíptica o conjunto

$$\mathrm{End}(E) = \mathrm{Hom}(E,E)$$

é um anel com a mesma adição acima e cuja multiplicação é dada pela composição

$$(\phi\psi)(P) = \phi(\psi(P))$$

$\mathrm{End}(E)$ é conhecido como o *anel de endomorfismos de* E. Os elementos invertíveis de $\mathrm{End}(E)$ formam o *grupo de automorfismos de* E, $\mathrm{Aut}(E)$. É claro que se E_1, E_2 e E estão definidas sobre um corpo K, então podemos restringir a nossa atenção as isogenias definidas sobre K. Elas também formam grupos que denotaremos por

$$\mathrm{Hom}_K(E_1,E_2) \qquad \mathrm{End}_K(E) \qquad \mathrm{Aut}_K(E)$$

Exemplo 3.1 *Multiplicação por m* - Se E/K é uma curva elíptica e m é um inteiro podemos definir um endomorfismo bastante natural, *a multiplicação por m*, definida da única maneira possível

$$\begin{array}{rcl} [m] : E & \longrightarrow & E \\ P & \longmapsto & [m]P \end{array}$$

Quando $m = 0$ temos a zero isogenia $[0]P = O$, já definida anteriormente. Que $[m]$ é uma isogenia segue, por indução, do fato de que a soma é um morfismo. Observemos que, neste caso, $[m]$ está definido sobre K, sempre que E estiver.

Para uma curva elíptica qualquer, o único exemplo óbvio de isogenias são estes, por isso eles são de vital importância para o estudo das curvas elípticas. Mais adiante desenvolveremos ferramentas que nos permitirão obter os seguintes resultados que ora enunciamos sem demonstração:

Teorema 3.4.2 *Sejam E/K uma curva elíptica e m um inteiro não nulo que não divide a característica de K. Então a multiplicação por m, $[m]$, é uma isogenia não constante com* $\deg[m] = m^2$.
Prova: (**3.4.12**, pg. 87) e (**4.1.2**, pg. 91) □

Vejamos que informações podemos obter deste resultado.

Consideremos duas curvas elípticas E_1 e E_2. Usando a composição de morfismo, podemos dotar $\mathrm{Hom}(E_1, E_2)$ de uma estrutura de $\mathbb{Z}$-módulo:

$$\begin{array}{rcl} \cdot : \mathbb{Z} \times \mathrm{Hom}(E_1, E_2) & \longrightarrow & \mathrm{Hom}(E_1, E_2) \\ (m, \phi) & \longmapsto & m \cdot \phi = [m] \circ \phi \end{array}$$

Se tivermos $m \cdot \phi = [0]$ então

$$m \cdot \phi = [m] \circ \phi = [0] \Longrightarrow \deg[m] \deg \phi = 0$$

Donde $m \neq 0 \Longrightarrow \deg[m] = m^2 > 0$, e daí $\deg \phi = 0$, ou equivalentemente, $\phi = [0]$.

Tomando $E = E_1 = E_2$, mostramos acima que $\mathrm{End}(E)$ é um anel de característica zero. Além do mais, se, para $\phi, \psi \in \mathrm{End}(E)$, tivermos $\phi \circ \psi = [0]$ então

$$\deg \phi \deg \psi = 0$$

ou seja

$$\phi = [0] \text{ ou } \psi = [0]$$

Donde

Corolário 3.4.3 *Sejam E_1, E_2 e E curvas elípticas. Então* $\mathrm{Hom}(E_1, E_2)$ *é um $\mathbb{Z}$-módulo livre de torção e* $\mathrm{End}(E)$ *é um domínio de integridade de característica zero.*
□

Nas seções vindouras, veremos que uma curva elíptica definida sobre $\mathbb{Q}$, por ser um grupo abeliano finitamente gerado, satisfaz

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \times \mathbb{Z}^r$$

O número r é chamado de *posto* de uma curva elíptica e E_{tors} é o *subgrupo de torção de E*, isto é, o conjunto dos pontos de E que possuem ordem finita. É útil

definirmos o subgrupo de *m-torção de* E, denotado por $E[m]$, formado pelos pontos que possuem ordem m. Em termos do mapa multiplicação por m temos:

$$E[m] = \ker[m] = \{P \in E \mid [m]P = O\}$$

O subgrupo de torção, se usarmos esta notação, será então escrito como

$$E_{tors} = \bigcup_{m=1}^{\infty} E[m].$$

Se E estiver definida sobre K, então $E_{tors}(K)$ denotará os pontos de ordem finita em $E(K)$.

Em uma curva elíptica E/K existe um homomorfismo natural de grupos $[\ ] : \mathbb{Z} \to \mathrm{End}(E)$. Diremos que a curva possui *multiplicação complexa* caso este homomorfismo não seja sobrejetivo, isto é, existam mais endomorfismos além das multiplicações por m.

A curva E/K, $\mathrm{char}(K) \neq 2$, definida por $y^2 = x^3 - x$ é um exemplo clássico de uma curva com multiplicação complexa, pois $\mathrm{End}(E)$ possui um mapa que não é uma multiplicação por m, denotado por $[i]$ e definido por

$$(x, y) \longmapsto (-x, iy)$$

onde $i \in \bar{K}$ é uma raiz quarta primitiva da unidade. Ademais $[i] \in \mathrm{End}_K(E)$ se, e só se, $i \in K$, mostrando-nos que podemos ter $\mathrm{End}_K(E) \subsetneq \mathrm{End}(E)$, ainda que E esteja definida sobre K. Como, para esta curva, temos $-(x, y) = (x, -y)$ então $[i] \circ [i] = [-1]$; o que nos dá um homomorfismo de anéis

$$\begin{array}{ccc} \mathbb{Z}[i] & \longrightarrow & \mathrm{End}(E) \\ m + ni & \longmapsto & [m] + [n] \circ [i] \end{array}$$

Outro exemplo clássico de mapas entre curvas elípticas relaciona as curvas

$$E_1 : y^2 = x^3 + ax^2 + bx$$
$$E_2 : Y^2 = X^3 - 2aX + rX$$

onde $\mathrm{char}(K) \neq 2$, $a, b \in K$, $b \neq 0$ e $r = a^2 - 4b \neq 0$. Usando a homogeneidade das coordenadas, as definições das curvas e o fato de elas serem lisas, mostra-se

facilmente que os mapas racionais abaixo são isogenias

$$\begin{array}{ccc} \phi : E_1 & \longrightarrow & E_2 \\ (x:y:1) & \longmapsto & (\dfrac{y^2}{x^2} : \dfrac{y(b-x^2)}{x^2} : 1) \end{array} \qquad \begin{array}{ccc} \hat{\phi} : E_2 & \longrightarrow & E_1 \\ (X:Y:1) & \longmapsto & (\dfrac{Y^2}{4X^2} : \dfrac{Y(r-X^2)}{8X^2} : 1) \end{array}$$

que satisfazem

$$\phi \circ \hat{\phi} = [2] : E_2 \to E_2 \qquad \text{e} \qquad \hat{\phi} \circ \phi = [2] : E_1 \to E_1$$

Este é caso particular de algo que mais adiante discutiremos: *Isogenia dual*. A isogenia dual permite, entre outras coisas, obter uma cota para a quantidade de pontos de uma curva elíptica sobre um corpo finito. Se K é um corpo tal que $\text{card}(K) = q < \infty$ então a cota, conjecturada por Artin e demonstrada por Hasse, é

$$|\#E(K) - q - 1| \leq 2\sqrt{q}$$

Crucial na obtenção desta cota é a seguinte isogenia

Exemplo 3.2 *O morfismo de Frobenius* - Sejam K um corpo de característica $p > 0$ e $q = p^r$. Suponhamos que uma curva elíptica E/K seja dada pela equação de Weierstrass

$$Y^3 + a_1XY + a_2Y - X^3 - a_2X^2 - a_4X - a_6$$

A partir desta equação podemos definir uma outra curva dada pelo polinômio

$$E^{(q)} : Y^3 + a_1^qXY + a_3^qY - X^3 - a_2^qX^2 - a_4^qX - a_6^q$$

Existe um morfismo entre estas duas curvas, chamado de *q-ésimo morfismo de Frobenius*, dado por

$$\begin{array}{ccc} \phi_q : E & \longrightarrow & E^{(q)} \\ (x,y) & \longmapsto & (x^q, y^q) \end{array}$$

O morfismo de Frobenius será uma isogenia se $E^{(q)}$ for uma curva elíptica; por sua vez, $E^{(q)}$ (curva dada por uma equação de Weierstrass) será uma curva elíptica se, e somente se, $\Delta(E^{(q)}) \neq 0$. Como num corpo de característica p vale $(a+b)^p = a^p + b^p$ temos, a partir de um simples cálculo, que

$$\Delta(E^{(q)}) = \Delta(E)^q \neq 0$$

Quando $K = \mathbb{F}_q$ é um corpo finito, então $a^p = a$, $\forall a \in K$ e o q-ésimo mapa de Frobenius sobre K será a identidade. Logo $E^{(q)} = E$ e ϕ_q é um endomorfismo de E, chamado de *endomorfismo de Frobenius*. Este endomorfismo goza das seguintes propriedades:

Teorema 3.4.4 *Seja K um corpo perfeito de característica $p > 0$ e $q = p^r$. Consideremos o q-ésimo morfismo de Frobenius $\phi : E \to E^{(q)}$ onde E/K e $E^{(q)}$ são curvas elípticas. Então:*
(a) $\phi^*(K(E^q)) = K(E)^q := \{f^q \mid f \in K(E)\}$,
(b) ϕ *é puramente inseparável,*
(c) $\deg \phi = q$.
Prova: [SILVERMAN], pg 30. □

Corolário 3.4.5 *Toda isogenia $\psi : E_1 \to E_2$ sobre um corpo de característica $p > 0$ se fatora como*

$$E_1 \xrightarrow{\phi} E_1^{(q)} \xrightarrow{\lambda} E_2$$

onde $q = \deg_i \psi$, ϕ é o q-ésimo morfismo de Frobenius e λ é separável.
Prova: [SILVERMAN], pg 30. □

Faremos agora um pouco de "Teoria de Galois" para curvas elípticas, isto é, resultados sobre curvas elípticas bastante semelhantes aos da Teoria de Galois. Para tanto necessitamos dos seguintes mapas definidos para uma curva elíptica E/K e para cada ponto $Q \in E$

$$\begin{array}{ccc} \tau_Q : E & \longrightarrow & E \\ P & \longmapsto & \tau_Q(P) = P + Q \end{array}$$

Este mapa é conhecido por *translação por Q*. Note que apesar de ser um isomorfismo (τ_Q possui uma inversa: τ_{-Q}) a translação por Q não é uma isogenia a menos que $Q = O$, pois $\tau_Q(O) = Q$.

Seja $F : E_1 \to E_2$ um morfismo qualquer entre curvas elípticas. O morfismo

$$\phi = \tau_{-F(O_1)} \circ F$$

satisfaz $\phi(O_1) = O_2$, logo é uma isogenia. E como

$$F = \tau_{F(O)} \circ \phi$$

vemos que todo mapa entre curvas elípticas pode ser decomposto por uma translação e uma isogenia.

Comecemos pelo seguinte resultado preparatório para os demais.

Teorema 3.4.6 *Seja $\phi : E_1 \to E_2$ uma isogenia não nula. Então*
(a) $\ker \phi$ *é um subgrupo finito de* E_1*;*
(b) Para todo $Q \in E_2$*,*

$$\#\phi^{-1}(Q) = \deg_s \phi$$

(c) O mapa

$$\begin{array}{rccc} \Lambda : \ker \phi & \longrightarrow & \mathrm{Aut}[\bar{K}(E_1)/\phi^*(\bar{K}(E_2))] \\ T & \longmapsto & \tau_T^* \end{array}$$

é um isomorfismo (onde τ_T^* *é o automorfismo em* $\bar{K}(E_1)$ *induzido por* τ_T*).*
(d) Para toda isogenia separável ϕ *se tem:* ϕ *não-ramificado,*

$$\#\ker \phi = \deg \phi$$

e $\bar{K}(E_1)$ *é uma extensão galoisiana de* $\phi^*(\bar{K}(E_1))$*.*
Prova: (a) $\ker \phi$ é um grupo pois ϕ é um homomorfismo de grupos. Além do mais para todo $Q \in E_2$ temos

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi$$

ou seja, $\phi^{-1}(Q)$ é finito para todo Q em E_2.

(b) Sabemos (**1.2.7**, pg. 15) que

$$\#\phi^{-1}(Q) = \deg_s \phi$$

exceto para um número finito de $Q \in E_2$. Seja $Q' \in E_2$ um ponto que satisfaça esta igualdade e seja Q um ponto qualquer de E_2. Como ϕ é sobrejetiva, considere o ponto $R_Q \in E_1$ tal que $\phi(R_Q) = Q' - Q$.

Então para $P \in \phi^{-1}(Q)$ temos que

$$\phi(P + R) = \phi(P) + \phi(R) = Q + Q' - Q = Q'$$

Logo existe uma correspondência

$$\begin{array}{ccc} \phi^{-1}(Q) & \longrightarrow & \phi^{-1}(Q') \\ P & \longmapsto & P + R \end{array}$$

obviamente bijetiva. Portanto, para todo $Q \in E_2$

$$\#\phi^{-1}(Q) = \#\phi^{-1}(Q') = \deg_s \phi$$

Observemos que se $T \in \ker \phi$ então $\phi \circ \tau_T = \phi$. Daí, para $P, P' \in \phi^{-1}(Q)$ temos $\phi \circ \tau_{P-P'} = \phi$ o que nos leva a concluir que

$$e_\phi(P') = e_{\phi\circ\tau_{P-P'}}(P') = e_\phi(\tau_{P-P'}(P'))e_{\tau_{P-P'}}(P') = e_\phi(P)$$

já que uma translação é um isomorfismo. Mostramos assim que todo ponto numa mesma fibra $\phi^{-1}(Q)$ tem o mesmo índice de ramificação. Logo

$$\begin{aligned}
\deg_s \phi \cdot \deg_i \phi &= \deg \phi \\
&= \sum_{P\in\phi^{-1}(Q)} e_\phi(P) \\
&= \#\phi^{-1}(Q) \cdot e_\phi(P) \\
&= \deg_s \phi \cdot e_\phi(P) \\
&\Downarrow \\
\deg_i \phi &= e_\phi(P), \text{ para } P \in \phi^{-1}(Q)
\end{aligned}$$

Como o Q é arbitrário, o resultado segue.

(c) Para $T \in \ker \phi$ vimos que $\phi \circ \tau_T = \phi$. Portanto se $f \in \bar{K}(E_2)$ então

$$\tau_T^*(\phi^*(f)) = \tau_T^*(f \circ \phi) = (f \circ \phi) \circ \tau_T = (\phi \circ \tau_T)^*(f) = \phi^*(f)$$

Isto significa que os elementos de $\phi^*(\bar{K}(E_2)$ são fixados por τ_T^* quando olhado como automorfismo de $\bar{K}(E_1)$, ou seja, o mapa Λ está bem definido. Λ também satisfaz, $\forall f \in \bar{K}(E_1)$

$$\begin{aligned}
\Lambda(S+T)(f) &= \tau_{T+S}^*(f) = f \circ \tau_{T+S} \\
&= f \circ (\tau_T \circ \tau_S) = (f \circ \tau_T) \circ \tau_S \\
&= \tau_S^*(f \circ \tau_T) = \tau_S^*(\tau_T^*(f)) \\
&= (\tau_S^* \circ \tau_T^*)(f) = (\Lambda(S) \circ \Lambda(T))(f)
\end{aligned}$$

isto é

$$\Lambda(S+T) = \Lambda(S) \circ \Lambda(T)$$

e Λ é um homomorfismo de grupos. Do item (b) e da teoria básica de Galois obtemos

$$\#\operatorname{Aut}[\bar{K}(E_1)/\phi^*(\bar{K}(E_2))] \leq \deg_s \phi = \#\ker\phi$$

Como Λ é um mapa entre conjuntos finitos onde a cardinalidade do contra-domínio é menor ou igual que a do domínio é suficiente mostrar que Λ é injetivo, para que ele seja um isomorfismo. Suponha então que $\tau_T^* \equiv \mathrm{Id}_{\bar{K}(E_1)}$. Ou equivalentemente $\forall f \in \bar{K}(E_1)$ temos

$$\begin{array}{rcl} \tau_T^*(f) & = & f \\ f(P+T) & = & f(P) \\ & \Downarrow & \\ f(T) & = & f(O) \end{array}$$

e evidentemente $T = O$

(d) Se ϕ é separável, então, utilizando o item (b), obtemos

$$\#\phi^{-1}(Q) = \deg\phi$$

e por (**1.2.8**, pg. 15) isto implica que ϕ é não ramificado. Esta última igualdade para $Q = O$ nos diz que

$$\ker\phi = \#\phi^{-1}(O) = \deg\phi$$

e de (b) chegamos a

$$\#\operatorname{Aut}[\bar{K}(E_1)/\phi^*(\bar{K}(E_2))] = \ker\phi = \deg\phi = [\bar{K}(E_1)/\phi^*(\bar{K}(E_2))]$$

Portanto a extensão $\bar{K}(E_1)/\phi^*(\bar{K}(E_2))$ é galoisiana. □

Corolário 3.4.7 *Sejam*

$$\phi : E_1 \to E_2 \qquad e \qquad \psi : E_1 \to E_3$$

isogenias não constantes, com ϕ separável. Se

$$\ker\phi \subset \ker\psi$$

então existe uma única isogenia $\lambda : E_2 \to E_3$ *tal que* $\psi = \lambda \circ \phi$
Prova: Uma vez que ϕ é separável, o resultado anterior nos garante que

$$\bar{K}(E_1)/\phi^*(\bar{K}(E_2))$$

é uma extensão galoisiana. Portanto a inclusão $\ker\phi \subset \ker\psi$ e o item (c) do resultado anterior nos diz que

$$\mathrm{Gal}(\bar{K}(E_1)/\phi^*(\bar{K}(E_2))) \simeq \ker\phi \subset \ker\psi \simeq \mathrm{Aut}[\bar{K}(E_1)/\psi^*(\bar{K}(E_2))]$$

Logo os elementos de $\mathrm{Gal}(\bar{K}(E_1)/\phi^*(\bar{K}(E_2)))$ fixam $\psi^*(\bar{K}(E_3))$ e temos claramente a seguinte inclusões de corpos

$$\psi^*(\bar{K}(E_3)) \subset \phi^*(\bar{K}(E_2)) \subset \bar{K}(E_1)$$

que podemos escrever a partir do seguintes mapas injetivos

$$\bar{K}(E_3) \xrightarrow{\psi^*} \phi^*(\bar{K}(E_2)) \xrightarrow{(\phi^*)^{-1}} \bar{K}(E_2)$$

Portanto (**1.2.5**, pg. 14) existe um morfismo

$$\lambda : E_2 \to E_3$$

tal que

$$\lambda^* = (\phi^*)^{-1} \circ \psi^* \Longrightarrow \psi^* = \phi^* \circ \lambda^*$$

Donde concluímos que

$$\psi = \lambda \circ \phi$$

Finalmente λ é uma isogenia pois satisfaz

$$\lambda(O_2) = \lambda(\phi(O_1)) = \psi(O_1) = O_3$$

□

Teorema 3.4.8 *Sejam* E *uma curva elíptica e* Φ *um subgrupo finito de* E*. Então existe uma única curva elíptica* E' *e uma isogenia separável*

$$\phi : E \to E'$$

tal que

$$\ker\phi = \Phi$$

Prova: Como na letra (b) do teorema anterior, cada ponto $T \in \Phi$ dá origem a um automorfismo $\tau_T^* \in \bar{K}(E)$. Seja $\bar{K}(E)^\Phi$ o corpo fixo de Φ em $\bar{K}(E)$. Portanto a Teoria de Galois nos diz que a extensão $\bar{K}(E)/\bar{K}(E)^\Phi$ é galoisiana e $\mathrm{Gal}(\bar{K}(E)/\bar{K}(E)^\Phi) = \Phi$.

$\bar{K}(E)/\bar{K}(E)^\Phi$ por ser galoisiana é finita, e conseqüentemente $\bar{K}(E)/\bar{K}$ tem grau de transcendência 1. Portanto (**1.2.5**, pg. 14) existe uma única curva lisa $E'/\bar{K}$ e um morfismo finito

$$\phi : E \to E'$$

tal que

$$\phi^*(\bar{K}(E')) = \bar{K}(E)^\Phi$$

Considere $P \in E$ e $T \in \Phi$. Como τ_T^* fixa todo elemento de $\phi^*\bar{K}(E') = \bar{K}(E)^\Phi$ temos, para toda função $f \in \bar{K}(E')$

$$f(\phi(T+P)) = f \circ \phi \circ \tau_T(P) = ((\tau_T^* \circ \phi^*)f)(P) = (\phi^* f)(P) = f(\phi(P))$$

Portanto $\phi(P+T) = \phi(P)$, $\forall T \in \Phi$. Além disso

$$\phi^{-1}(Q) \supset \{P + T \mid T \in \Phi\}$$

para todo $Q \in C$ e todo $P \in \phi^{-1}(Q)$. Observemos que quando fixamos P e fazemos T percorrer o conjunto Φ, os elementos $P+T$ são todos distintos e, portanto, $\#\{P+T \mid T \in \Phi\} = \#\Phi$. Assim, a inclusão acima nos diz que

$$\#\phi^{-1}(Q) \geq \#\Phi = \deg \phi$$

Por outro lado temos

$$\#\phi^{-1}(Q) = \deg_s \phi \leq \deg \phi$$

Daí

$$\#\phi^{-1}(Q) = \deg \phi, \quad \forall Q \in E$$

ou, equivalentemente, ϕ é não ramificado.

A fórmula de Hurwitz (**1.5.6**, pg. 22), para um mapa ϕ não ramificado, implica que

$$\begin{array}{rcl} 2\text{gênero}(E) - 2 & = & \deg \phi (2\text{gênero}(E') - 2) \\ & \Downarrow & \\ \text{gênero}(E') & = & 1 \end{array}$$

uma vez que gênero$(E) = 1$. Portanto E' é uma curva elíptica e ϕ torna-se uma isogenia quando tomamos $\phi(O_E)$ como elemento neutro. $\square$

Sendo assim, considere o invariante diferencial de uma curva elíptica E/K

$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y} \in \Omega_E$$

onde E é dada pela seguinte equação de Weierstrass

$$Y^3 + a_1XY + a_2Y - X^3 - a_2X^2 - a_4X - a_6$$

A primeira propriedade importante de ω e o motivo pelo qual ele é chamado de invariante diferencial é a seguinte

Teorema 3.4.9 *Seja E uma curva elíptica. Então o invariante diferencial ω associado a uma equação de Weierstrass para E satisfaz*

$$\tau_Q^*(\omega) = \omega, \qquad \forall Q \in E$$

(Aqui, τ_Q é a translação por Q)
Prova: Sabemos que $\operatorname{div}(\omega)$, por ser o divisor de uma diferencial, é um divisor canônico, logo pelo Riemann-Roch (**1.5.4**, pg. 22)

$$\ell(\operatorname{div}(\omega)) = 1 \qquad \text{e} \qquad f \in \mathcal{L}(\operatorname{div}(\omega)) \Longrightarrow \operatorname{div}(f) = 0$$

e da definição de $\mathcal{L}(\operatorname{div}(\omega))$ temos que

$$\operatorname{div}(f) \geq -\operatorname{div}(\omega) \Longrightarrow \operatorname{div}(\omega) \geq 0.$$

Em outras palavras, ω é holomorfo.

Suponhamos que ω' seja outro diferencial holomorfo. Logo, como Ω_E é unidimensional (**1.4.1**, pg. 18), existe $f \in \bar{K}(E)$ tal que

$$\begin{array}{rcl}
\omega' & = & f\omega \\
 & \Downarrow & \\
\operatorname{div}(\omega') & = & \operatorname{div}(f) + \operatorname{div}(\omega) \\
\operatorname{div}(f) & = & \operatorname{div}(\omega') - \operatorname{div}(\omega) \\
 & \geq & -\operatorname{div}(\omega) \quad (\omega' \text{ é holomorfo}) \\
 & \Downarrow & \\
f \in \mathcal{L}(\operatorname{div}(\omega)) & \Longrightarrow & f \in K
\end{array}$$

ou seja, o diferencial holomorfo é único a menos de uma constante.

O diferencial $\tau_Q^*(\omega)$ é holomorfo, pois temos que (**1.3.2**, pg. 18)

$$\mathrm{div}(\tau_Q^*(\omega)) = \tau_Q^*(\mathrm{div}(\omega)) \geq 0.$$

(A desigualdade torna-se clara ao usarmos a definição de τ_Q^*)

Daí existe uma constante $a \in K$ tal que

$$\tau_Q^*(\omega) = a\omega, \qquad \forall Q \in E$$

Se fizermos $Q = O$ na igualdade acima achamos $a = 1$ e portanto segue o resultado. □

Este fato permite simplificar bastante a demonstração do próximo teorema que mostra um resultado bastante conhecido da Análise: diferenciar é linearizar!

Teorema 3.4.10 *Sejam E e E' duas curvas elípticas, ω o invariante diferencial de E e $\phi, \psi : E' \to E$ duas isogenias. Então*

$$(\phi + \psi)^*(\omega) = \phi^*(\omega) + \psi^*(\omega)$$

Prova: Para $\phi = [0]$ ou $\psi = [0]$ não há o que demonstrar. Caso $\phi + \psi = [0]$, então usando o fato de que

$$\psi^* = (-\phi)^* = \phi^* \circ [-1]^*$$

resta-nos mostrar que

$$[-1]^*(\omega) = -\omega.$$

Como

$$-(x, y) = (x, -y - a_1x - a_3)$$

segue que

$$\begin{aligned} [-1]^*(\omega) &= [-1]^*\left(\frac{dx}{2y + a_1x + a_3}\right) = \frac{d(x \circ [-1])}{y \circ [-1] + a_1x \circ [-1] + a_3} \\ &= \frac{dx}{2(-y - a_1x - a_3) + a_1x + a_3} \\ &= -\omega. \end{aligned}$$

Portanto podemos assumir que ϕ, ψ e $\phi + \psi$ são todos não constantes e considerar (x_1, y_1) e (x_2, y_2) duas coordenadas de Weierstrass para E independentes, no sentido de que elas satisfazem a equação de Weierstrass mas nenhuma outra relação algébrica.

Considere

$$(x_3, y_3) = \underbrace{(x_1, y_1)}_{P_1} + \underbrace{(x_2, y_2)}_{P_2}$$

então a fórmula de adição de pontos nos diz que x_3 e y_3 são combinações racionais de x_1, x_2, y_1 e y_2. Para qualquer (x, y) denotaremos por $\omega(x, y)$ o diferencial invariante correspondente

$$\omega(x, y) = \frac{dx}{2y + a_1 x + a_3}.$$

Desta forma temos que

$$\omega(x_3, y_3) = f(x_1, y_1, x_2, y_2)\omega(x_1, y_1) + g(x_1, y_1, x_2, y_2)\omega(x_2, y_2)$$

onde f e g são funções racionais de x_1, y_1, x_2 e y_2. Esta última igualdade provém da fórmula para a adicão de pontos, das regras usuais de diferenciação e da relação $(2y_i + a_1 x_i + a_3)dy_i = (3x_i^2 + 2a_2 x_i + a_4 - a_1 y_i)dx_i$ obtida do fato de que x_i e y_i satisfazem a equação de Weierstrass dada. Mostraremos que f e g são identicamente 1, usando para isso o fato de ω ser invariante por translação.

Escolhamos um ponto qualquer de E, digamos Q, e ponhamos

$$x_2 = x(Q) \qquad \text{e} \qquad y_2 = y(Q).$$

Então

$$dx_2 = d_x(Q) = 0 \qquad \text{e} \qquad \text{portanto } \omega(x_2, y_2) = 0.$$

Desta forma escreveremos $\omega(x_3, y_3)$ como

$$\begin{aligned} \omega(x_3, y_3) &= \frac{d(x(P_1 + Q))}{y(P_1 + Q) + a_1 x(P_1 + Q) + a_3} \\ &= \tau_Q^*(\omega(x_1, y_1)) \\ &= \omega(x_1, y_1). \end{aligned}$$

Substituindo esta igualdade na expressão acima que nos dá $\omega(x_3, y_3)$ como uma combinação racional de $\omega(x_1, y_1)$ obtemos

$$f(x_1, y_1, x(Q), y(Q)) \equiv 1$$

ao olharmos f como uma função racional em $\bar{K}(x_1, y_1)$. Como o ponto Q foi escolhido arbitrariamente, teremos que f é uma função identicamente 1. Invertendo os papéis entre (x_1, y_1) e (x_2, y_2), vê-se que $g \equiv 1$. Mostrando assim que se

$$(x_3, y_3) = (x_1, y_2) + (x_2, y_2)$$

então

$$\omega(x_3, y_3) = \omega(x_1, y_1) + \omega(x_2, y_2).$$

Seja (x', y') uma coordenada de Weierstrass sobre E'. Coloquemos

$$\begin{aligned} x_1 &= x(\phi(x', y')) \\ y_1 &= y(\phi(x', y')) \\ x_2 &= x(\psi(x', y')) \\ y_2 &= y(\psi(x', y')) \\ x_3 &= x(\phi + \psi)(x', y')) \\ y_3 &= y(\phi + \psi)(x', y')) \end{aligned}$$

ou melhor

$$\begin{aligned} (\phi + \psi)(x', y') &= \phi(x', y') + \psi(x', y') \\ (x_3, y_3) &= (x_1, y_1) + (x_2, y_2) \\ &\Downarrow \\ \omega(x_3, y_3) &= \omega(x_1, y_1) + \omega(x_2, y_2) \\ &\Downarrow \\ (\phi + \psi)^*(\omega) &= \phi^*(\omega) + \psi^*(\omega). \end{aligned}$$

□

Corolário 3.4.11 *Sejam ω o invariante diferencial sobre uma curva elíptica E e m um inteiro. Então*

$$[m]^*(\omega) = m\omega$$

Prova: Indução sobre m. □

Corolário 3.4.12 *Sejam E/K uma curva elíptica e m um inteiro não nulo. Assuma que* $\mathrm{char}(K) = 0$ *ou que m é relativamente primo a* $\mathrm{char}(K)$. *Então a multiplicação por m é um endomorfismo não constante e separável.*
Prova: O invariante diferencial em E, ω, satisfaz

$$[m]^*(\omega) = m\omega \neq 0$$

e logo $[m]$ é não constante. Como o mapa $[m]^*$ é injetivo então, por (**1.4.2**, pg. 19) $[m]$ é separável. □

Capítulo 4

Isogenia dual e corpos finitos

4.1 A isogenia dual

As ferramentas desenvolvidas nesta seção permitirão mostrar que para uma curva elíptica E/K, $\#K = q$, temos

$$|\#E(K) - q - 1| \leq 2\sqrt{q}.$$

Este resultado foi conjecturado por E. Artin em sua tese e recebeu uma demonstração na década de 30 por Hasse. Essa demonstração utiliza a noção de isogenia dual que surge naturalmente do seguinte fato.

Consideremos uma isogenia $\phi : E_1 \to E_2$ não constante. Então ϕ induz um mapa

$$\phi^* : \mathrm{Pic}^0(E_2) \to \mathrm{Pic}^0(E_1).$$

Por outro lado, existem isomorfismos

$$\kappa_i : E_i \to \mathrm{Pic}^0(E_i)$$

que resultam num homomorfismo de E_2 em E_1, a saber

$$E_2 \xrightarrow{\kappa_2} \mathrm{Pic}^0(E_2) \xrightarrow{\phi^*} \mathrm{Pic}^0(E_1) \xrightarrow{\kappa_1^{-1}} E_1 \cdot$$

E surpreendentemente existe uma isogenia que, como homomorfismo de grupos, coincide com a aplicação anterior.

Teorema 4.1.1 *Seja $\phi : E_1 \to E_2$ uma isogenia não constante de grau m.*

(a) Então existe uma única isogenia

$$\hat{\phi} : E_2 \to E_1$$

tal que

$$\hat{\phi} \circ \phi = [m]$$

(b) Como homomorfismo de grupos $\hat{\phi}$ coincide com

$$E_2 \longrightarrow \mathrm{Div}^0(E_2) \xrightarrow{\phi^*} \mathrm{Div}^0(E_1) \xrightarrow{soma} E_1$$

$$Q \longmapsto (Q) - (O_2) \longmapsto \sum n_p(P) \longmapsto \sum [n_p]P$$

Prova: (a) Mostremos a unicidade. Suponha que $\hat{\phi}$ e $\hat{\phi}'$ são duas isogenias dentro das condições do teorema. Então

$$(\hat{\phi} - \hat{\phi}') \circ \phi = [m] - [m] = [0].$$

Como ϕ é não constante, segue que $\hat{\phi} - \hat{\phi}'$ é constante e, portanto, $\hat{\phi} = \hat{\phi}'$.

Observemos que se tivermos uma isogenia $\psi : E_2 \to E_1$, digamos $\deg \psi = n$, e supusermos que existam $\hat{\psi}$ e $\hat{\phi}$. Então

$$(\hat{\phi} \circ \hat{\psi}) \circ (\psi \circ \phi) = \hat{\phi} \circ [n] \circ \phi = [n] \circ \hat{\phi} \circ \phi = [n][m] = [nm].$$

Logo, pela unicidade mostrada acima, temos que

$$\widehat{\psi \circ \phi} = \hat{\phi} \circ \hat{\psi}.$$

Assim é suficiente mostramos a existência de $\hat{\phi}$ quando ϕ é separável ou é o morfismo de Frobenius, uma vez que todo morfismo entre curvas não singulares, em característica $p > 0$, é uma composição de um mapa separável e um morfismo de Frobenius e um morfismo em característica zero é sempre separável.

Suponhamos, inicialmente que ϕ é separável. Como $\deg \phi = m$, temos que

$$\# \ker \phi = m$$

e portanto

$$\ker \phi \subset \ker[m].$$

Logo existe um mapa (**3.4.7**, pg. 80)

$$\hat{\phi} : E_2 \to E_1$$

com $\hat{\phi} \circ \phi = [m]$.

Seja $q = p^e$. Se $\phi(x, y) = (x^q, y^q)$ é o q-ésimo morfismo de Frobenius então temos que

$$\phi(x, y) = \underbrace{(x^p, y^p) \circ (x^p, y^p) \circ ... \circ (x^p, y^p)}_{e \text{ vezes}} = \alpha^e$$

onde α representa o p-ésimo morfismo de Frobenius. Assim podemos supor que ϕ é o p-ésimo morfismo de Frobenius e que (**3.4.4**, pg. 77) $\deg \phi = p$.

Consideremos o invariante diferencial ω e o que lhe acontece ao aplicarmos $[p]^*$. Pelo que vimos

$$[p]^*\omega = p\omega = 0$$

já que K tem característica p. Como $[p]^*$ não é injetivo podemos concluir (**1.4.2**, pg. 19) que $[p]$ é um mapa não separável e que o mapa ϕ aparece realmente em sua decomposicão como um mapa separável e um morfismo de Frobenius (**3.4.5**, pg. 77). Em outras palavras, existe um morfismo separável ψ tal que

$$[p] = \psi \circ \phi^t$$

para algum inteiro $t \geq 1$. Ao tomarmos

$$\hat{\phi} = \psi \circ \phi^{t-1}$$

obteremos o resultado desejado.

(b) Considere um ponto Q de E_2. Para este ponto temos

$$\begin{aligned}
\text{soma}(\phi^*((Q) - (O_2))) &= \sum_{P \in \phi^{-1}(Q)} [e_\phi(P)]P - \sum_{T \in \ker \phi} [e_\phi(T)]T \\
&= [\deg_i \phi](\sum_{P \in \phi^{-1}} P - \sum_{T \in \ker \phi} T) \\
&= [\deg_i \phi]([\#\phi^{-1}(Q)]P - [\#\ker \phi]T) \\
&= [\deg_i \phi][\deg_s \phi](P - T) \\
&= [\deg \phi](P - T).
\end{aligned}$$

Observemos que os conjuntos $\{P - T \mid T \in \ker \phi, P \in \phi^{-1}\}$ e $\phi^{-1}(Q)$ são iguais. Daí

$$\begin{aligned} \text{soma}(\phi^*((Q) - (O_2)) &= [\deg \phi]P, \text{ para qualquer } P \in \phi^{-1}(Q) \\ &= \hat{\phi} \circ \phi(P) \\ &= \hat{\phi}(Q). \end{aligned}$$

□

Para uma isogenia não constante $\phi : E_1 \to E_2$ a isogenia $\hat{\phi} : E_2 \to E_1$ dada pelo teorema anterior é chamada de *a isogenia dual de* ϕ. Quando $\phi = [0]$ convenciona-se tomar $\hat{\phi} = [0]$. A isogenia dual satisfaz

Teorema 4.1.2 *Seja* $\phi : E_1 \to E_2$ *uma isogenia com* $\deg \phi = m$. *Então*

(a)

$$\begin{aligned} \hat{\phi} \circ \phi &= [m] : E_1 \to E_1 \\ \phi \circ \hat{\phi} &= [m] : E_2 \to E_2 \end{aligned}$$

(b) $\widehat{\psi \circ \phi} = \hat{\phi} \circ \hat{\psi}$, *para toda isogenia* $\psi : E_2 \to E_3$.

(c) $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$, *para uma isogenia* $\psi : E_1 \to E_2$.

(d) $\forall m \in \mathbb{Z}$

$$\widehat{[m]} = [m] \qquad e \qquad \deg[m] = m^2$$

(e) $\deg \hat{\phi} = \deg \phi$.

(f) $\hat{\hat{\phi}} = \phi$.

Prova: O teorema é trivial para isogenias constantes, por isso suponhamos que todas as isogenias aqui tratadas são não constantes.

(a) A primeira parte é o teorema anterior. Para a segunda façamos

$$(\phi \circ \hat{\phi} - [m]) \circ \phi = \phi \circ \hat{\phi} \circ \phi - [m] \circ \phi = \phi \circ [m] - \phi \circ [m] = O.$$

Como ϕ é não constante, o mapa $\phi \circ \hat{\phi} - [m]$ será constante, obtendo assim o resultado desejado.

(b) Veja a parte inicial da demonstração do resultado anterior.

(c) Consideremos as seguintes coordenadas de Weierstrass para E_1 e E_2: $x_1, y_1 \in K(E_1)$ e $x_2, y_2 \in K(E_2)$. Pensemos em E_2 como uma curva elíptica definida sobre o corpo $K(E_1) = K(x_1, y_1)$. Assim dizer que ϕ é uma isogenia é o mesmo que dizer que $\phi(x_1, x_2) \in E_2/K(x_1, y_1)$ e afirmações semelhantes valem para $\phi + \psi$ e ψ.

Sabemos que $(\phi + \psi)(x_1, y_1) = \phi(x_1, y_1) + \psi(x_1, y_1)$ e portanto, como outrora observamos, temos que o divisor

$$D = ((\phi + \psi)(x_1, y_1)) - (\phi(x_1, y_1)) - (\psi(x_1, y_1)) + (O) \in \mathrm{Div}_{K(E_1)}(E_2)$$

é linearmente equivalente ao divisor nulo. Portanto existe uma função

$$f \in K(x_1, y_1)(E_2) = K(x_1, y_1, x_2, y_2) = K(x_2, y_2)(E_1)$$

que quando olhada como uma função de x_2, y_2 terá divisor D.

Mudemos o ponto de vista e consideremos f como uma função em $K(x_2, y_2)(E_1)$. Se $P_1 = (x_1, y_1) \in \overline{K(x_2, y_2)(E_1)}$ é um ponto satisfazendo $\phi(P_1) = (x_2, y_2)$ notemos que

$$f_1 \circ \phi(x_1, y_1) = f_1(x_2, y_2) = f(x_1, y_1, x_2, y_2) = f_2(x_1, y_1)$$

e então

$$\mathrm{ord}_{P_1}\ f = \mathrm{ord}_{P_1}\ f_2 = \mathrm{ord}_{P_1}\ f_1 \circ \phi = \mathrm{ord}_{P_1}\ f \circ \phi$$

e daí, se observarmos que (**1.2.7**, pg. 15)

$$\mathrm{ord}_{\phi(P_1)}\ f = -1 \qquad \text{e} \qquad \mathrm{ord}_{P_1}\ f \circ \phi = e_\phi(P_1) \cdot \mathrm{ord}_{\phi(P_1)}\ f$$

chegamos a seguinte conclusão

$$\mathrm{ord}_{P_1}\ f = -e_\phi(P_1).$$

De maneira análoga mostra-se que f terá um pólo de ordem $e_\psi(P_1)$ em P_1 e um zero de ordem $e_{\phi+\psi}(P_1)$ se pudermos concluir que $\psi(P_1) = (x_2, y_2)$ e $(\phi + \psi)(P_1) = (x_2, y_2)$, respectivamente. E assim, por exemplo,

$$\mathrm{ord}_{(x_2,y_2)}\ f = \sum_{P_1 \in \phi^{-1}(x_2,y_2)} \mathrm{ord}_{P_1}\ f = \sum_{P_1 \in \phi^{-1}(x_2,y_2)} e_\phi(P_1)$$

e conseqüentemente logramos o seguinte divisor para a função f quando olhada como uma função em x_1 e y_1

$$(\phi + \psi)^*((x_2, y_2)) - \phi^*((x_2, y_2)) - \psi^*((x_2, y_2)) + \sum n_i(P_i) \in \mathrm{Div}_{\overline{K(x_2,y_2)}}(E_1)$$

onde os P_i's estão em $E_1(\bar{K})$, já que pertencem a $\ker\phi$. Este divisor é linearmente equivalente ao divisor nulo e daí (**3.3.5**, pg. 65) tem soma igual a O

$$soma\{(\phi+\psi)^*((x_2,y_2)-(O))-\phi^*((x_2,y_2)-(O))-\psi^*((x_2,y_2)-(O))\} = -\sum[n_i]P_i'$$

com $P_i' \in E_1(\bar{K})$. O teorema antecedente, então nos garante que

$$\widehat{(\phi+\psi)}(x_2,y_2) - \hat{\phi}(x_2,y_2) - \hat{\psi}(x_2,y_2) = cte$$

já que não depende de (x_2,y_2), pois está em $E_1(\bar{K})$. Portanto ao tomarmos $(x_2,y_2) = O$ temos

$$\widehat{(\phi+\psi)}(O) - \hat{\phi}(O) - \hat{\psi}(O) = O - O - O$$

e claramente

$$\widehat{\phi+\psi} = \hat{\phi} + \hat{\psi}$$

(d) Para $m = 0, 1$ o resultado é óbvio.

$$\widehat{[m+1]} = \widehat{[m]+[1]} = \widehat{[m]} + \widehat{[1]} = [m] + [1] = [m+1]$$

e o resultado segue por indução.

Temos ainda que

$$[\deg[m]] = [m] \circ \widehat{[m]} = [m] \circ [m] = [m^2]$$

e como o anel de endomorfismo de uma curva elíptica é um $\mathbb{Z}$-módulo livre, segue que $\deg[m] = m^2$.

(e) Sabemos que

$$m^2 = \deg[m] = \deg(\hat{\phi}\circ\phi) = \deg\hat{\phi}\cdot\deg\phi = \deg\hat{\phi}\cdot m$$

e portanto

$$\deg\hat{\phi} = m$$

(f) Como a isogenia dual $\hat{\hat{\phi}}$ de $\hat{\phi}$ deve ser a *única* isogenia tal que

$$\hat{\phi}\circ\hat{\hat{\phi}} = [m]$$

e temos que

$$\hat{\phi}\circ\phi = [m]$$

então

$$\hat{\hat{\phi}} = \phi$$

□

Sejam A um grupo abeliano e $d : A \to \mathbb{R}$ uma funcão. d é uma *forma quadrática* em A se satisfaz:
(i) $d(a) = d(-a), \quad \forall a \in A$;
(ii) o mapa

$$\begin{array}{rccc} < , >: A \times A & \longrightarrow & \mathbb{R} \\ < a, b > & \longmapsto & d(a+b) - d(a) - d(b) \end{array}$$

é bilinear.

Diremos que uma forma quadrática d é *positiva definida* se
(iii) $d(a) \geq 0, \quad \forall a \in A$;
(iv) $d(a) = 0$ se, e só se, $a = e$ (elemento neutro).

A definicão acima e o teorema precedente nos dizem que

Corolário 4.1.3 *Seja E_1 e E_2 duas curvas elípticas. Então a aplicação*

$$\begin{array}{rccc} \deg : \mathrm{Hom}(E_1, E_2) & \longrightarrow & \mathbb{Z} \\ \phi & \longmapsto & \deg \phi \end{array}$$

é uma forma quadrática positiva definida.
Prova: Claramente

$$\deg([-1] \circ \phi) = \deg[-1] \deg \phi = \deg \phi$$

já que $[-1] \circ [-1]$ é um isomorfismo. Para mostrarmos que

$$< \phi, \psi >= \deg(\phi + \psi) - \deg \phi - \deg \psi$$

é bilinear usaremos a injeção

$$[\,] : \mathbb{Z} \to \mathrm{End}(E_1)$$

da seguinte maneira

$$\begin{array}{rcl} [< \phi, \psi >] & = & [\deg(\phi + \psi)] - [\deg \phi] - [\deg \psi] \\ & = & \widehat{(\phi + \psi)} \circ (\phi + \psi) - \hat{\phi} \circ \phi - \hat{\psi} \circ \psi \\ & = & (\hat{\phi} + \hat{\psi}) \circ (\phi + \psi) - \hat{\phi} \circ \phi - \hat{\psi} \circ \psi \\ & = & \hat{\phi} \circ \psi + \hat{\psi} \circ \phi \end{array}$$

Observe que esta última expressão é linear tanto em ϕ quanto em ψ e portanto $< , >$ é bilinear. As outras propriedades são triviais. □

4.2 A cota de Hasse

Vejamos como os resultados das seções anteriores permitem-nos obter a cota de Hasse. Para tanto necessitamos ainda do seguinte lema.

Lema 4.2.1 *Seja A um grupo abeliano e $d : A \to \mathbb{Z}$ uma forma quadrática positiva definida. Então para todo a e b em A temos*

$$|d(a+b) - d(a) - d(b)| \leq 2\sqrt{d(a) \cdot d(b)}.$$

Prova: Para $a = e$ ou $b = e$, não há o que se demonstrar; portanto assumiremos que $d(a)$ e $d(b)$ são não nulos.

Pela definicão de forma quadrática temos que o mapa

$$< a, b >= d(a+b) - d(a) - d(b)$$

é bilinear. Da positividade de d obtemos, para todo $m \in \mathbb{Z}$

$$0 \leq d(ma - b) = m^2 d(a) - mn < a, b > +d(b).$$

Entretanto para que esta inequação quadrática em m seja satisfeita, seu discriminante $< a, b >^2 -4d(a)d(b)$ deve ser não positivo e portanto

$$\begin{aligned} < a, b >^2 -4d(a)d(b) &\leq 0 \\ < a, b >^2 &\leq 4d(a)d(b) \\ |d(a+b) - d(a) - d(b)| &\leq 2\sqrt{d(a)d(b)} \end{aligned}$$

□

Teorema 4.2.2 *Seja E/K uma curva elíptica, $\#K = q$. Então*

$$|\#E(K) - q - 1| \leq 2\sqrt{q}.$$

Prova: Escolhamos uma equação de Weierstrass para E com coeficientes em K e consideremos o q-ésimo morfismo de Frobenius

$$\begin{array}{ccc} \phi : E & \longrightarrow & E \\ (x,y) & \longmapsto & (x^q, y^q) \end{array} .$$

Afirmamos que

1. $\phi(P) = P$, para todo $P \in E(K)$;
2. O endomorfismo $[1] - \phi$ é separável; e
3. $\deg : \mathrm{End}(E) \to \mathbb{Z}$ é uma forma quadrática positiva definida.

A terceira afirmação é o último resultado da seção anterior. Antes de demonstrarmos as duas primeiras, vejamos como elas implicam este resultado.

A afirmação 1 nos diz que

$$\ker([1] - \phi) = E(K)$$

enquanto que da afirmação 2 e (**3.4.6**, pg. 78) obtemos

$$\#E(K) = \#\ker([1] - \phi) = \deg_s([1] - \phi) = \deg([1] - \phi)$$

Por fim o lema anterior e a terceira afirmação nos diz exatamente que

$$|\#E(K) - \deg[1] - \deg\phi| \leq 2\sqrt{\deg[1] \cdot \deg\phi}$$

Agora para obtermos o resultado desejado é suficiente lembrar que $\deg\phi = q$ e $\deg[1] = 1$.

Seguem as demonstrações das afirmações 1 e 2

1. $\forall P \in E(K), \phi(P) = P$.
   Sabemos que
   $$P \in E(K) \iff P^\sigma = P, \forall \sigma \in G_{\bar{K}/K}$$
   A aplicação
   $$\begin{array}{ccc} \sigma_q : \bar{K} & \longrightarrow & \bar{K} \\ x & \longmapsto & \sigma_q(x) = x^q \end{array}$$
   claramente satisfaz $\sigma_q \in G_{\bar{K}/K}$. Portanto para $P = (x,y) \in E(K)$
   $$\phi(P) = (x^q, y^q) = (x,y)^{\sigma_q} = P$$

2. $[1] - \phi$ é separável.
   Aqui usaremos duplamente o fato (**1.4.2**, pg. 19): um morfismo $\theta : C \to C'$ é separável se, e só se, $\theta^* : \Omega_{C'} \to \Omega_C$ é injetivo. Ao aplicarmos isto ao mapa de ϕ Frobenius, por ser ele puramente inseparável (**3.4.4**, pg. 77), temos $\phi^*(\omega) = 0$, onde ω é o invariante diferencial de E. Daí

$$([1] - \phi)^*(\omega) = [1]^*(\omega) - \phi^*(\omega) = [1]^*(\omega) = \omega \neq 0$$

   e, mais uma aplicação do resultado citado acima, garante a separabilidade do mapa $[1] - \phi$.

□

Observemos que para curvas de gênero $g \geq 1$ vale a seguinte cota de Hasse-Weil

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2g\sqrt{q}.$$

Corolário 4.2.3 *Seja $\psi : E_1 \to E_2$ uma isogenia definida sobre $\mathbb{F}_q$. Então*

$$\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q).$$

Prova: Sejam ϕ_1 e ϕ_2 os q-ésimos endomorfismos de Frobenius em E_1 e E_2 respectivamente. Notemos que $\psi \circ \phi_1 = \phi_2 \circ \psi$, já que ψ está definida sobre $\mathbb{F}_q$ e portanto

$$\psi \circ ([1] - \phi_1) = ([1] - \phi_2) \circ \psi$$

e daí

$$\deg \psi \cdot \deg([1] - \phi_1) = \deg([1] - \phi_2) \deg \psi$$
$$\#E_1(\mathbb{F}_q) = \deg([1] - \phi_1) = \deg([1] - \phi_2) = \#E_2(\mathbb{F}_q)$$

□

Quando demonstramos que $\deg : \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$ é uma forma quadrática (**4.1.3**, pg. 94) obtivemos a seguinte igualdade

$$[< \phi, \psi >] = \hat{\phi} \circ \psi + \hat{\psi} \circ \phi$$

Consideremos um mapa $\phi \in \mathrm{End}(E)$. Ao aplicarmos esta igualdade ao mapa ϕ e $\psi = [1]$ obtemos

$$\hat{\phi} + \phi = [< \phi, [1] >] \in \mathbb{Z}$$

Ao número $< \phi, [1] >$ chamamos de *traço* de ϕ e indicamos por $\mathrm{Tr}(\phi)$. Podemos então definir o *polinômio característico de um mapa* ϕ por

$$c_\phi(T) = T^2 - \mathrm{Tr}(\phi)T + \deg \phi$$

Observemos que, pela propriedade característica da isogenia dual, o polinômio característico de ϕ satisfaz

$$\begin{aligned} c_\phi(\phi) &= \phi^2 - [\mathrm{Tr}(\phi)] \circ \phi + [\deg \phi] \\ &= \phi^2 - (\phi + \hat{\phi}) \circ \phi + [\deg \phi] \\ &= \phi^2 - \phi^2 - \hat{\phi} \circ \phi + [\deg \phi] \\ &= [0] \end{aligned}$$

e que para um número racional $r = m/n$ vale

$$\begin{aligned} c_\phi(r) &= (m/n)^2 - \mathrm{Tr}(\phi)m/n + \deg \phi \\ n^2 c_\phi(r) &= m^2 - mn\,\mathrm{Tr}(\phi) + n^2 \deg \phi \\ &= \deg([m] - [n] \circ \phi) \geq 0. \end{aligned}$$

Lema 4.2.4 *Sejam E uma curva elíptica e $\phi \in \mathrm{End}(E)$. O polinômio característico de ϕ, $c_\phi(T)$, satisfaz*
(a) $c_\phi(T) \in \mathbb{Z}[T]$;
(b) $c_\phi(\phi) = 0$;
(c) $c_\phi(r) \geq 0, \forall r \in \mathbb{Q}$, ou equivalentemente, as raízes complexas do polinômio característico não são reais. □

Lema 4.2.5 *Seja E uma curva elíptica e $\phi \in \mathrm{End}(E)$. Então existem α e β em $\bar{\mathbb{Q}}$ tais que, para todo natural m*

$$\mathrm{Tr}(\phi^m) = \alpha^m + \beta^m \qquad e \qquad \deg \phi^m = \alpha^m \beta^m$$

Prova:

Chamemos de α e β às raízes de $c_\phi(T)$ em $\bar{\mathbb{Q}}$. Logo

$$\alpha + \beta = \mathrm{Tr}\,\phi \qquad \text{e} \qquad \alpha\beta = \deg\phi$$

A relação seguinte vale sempre que $ab = ba$

$$a^{m+1} + b^{m+1} = (a+b)(a^m + b^m) - ab(a^{m-1} + b^{m-1}) \tag{4.1}$$

E dela segue facilmente por indução que $\alpha^m + \beta^m \in \mathbb{Z}, \forall m$. Logo, por mais uma indução em m temos (note que ϕ e $\hat{\phi}$ comutam, isto é, $\phi \circ \hat{\phi} = \hat{\phi} \circ \phi$)

$$\begin{aligned}
[\mathrm{Tr}\,\phi^{m+1}] &= \phi^{m+1} + \hat{\phi}^{m+1} \\
&= (\phi + \hat{\phi})(\phi^m + \hat{\phi}^m) - \phi \circ \hat{\phi}(\phi^{m-1} + \hat{\phi}^{m-1}) \\
&= [\mathrm{Tr}(\phi)][\mathrm{Tr}(\phi^m)] - [\deg\phi][\mathrm{Tr}(\phi^{m-1})] \\
\text{(hipótese de indução)} &= [(\alpha+\beta)][(\alpha^m + \beta^m)] - [\alpha\beta][(\alpha^{m-1} + \beta^{m-1})] \\
&= [\alpha^{m+1} + \beta^{m+1}]
\end{aligned}$$

□

Teorema 4.2.6 *Seja $e_n = \#E(\mathbb{F}_{q^n})$, $E/\mathbb{F}_q$ uma curva elíptica. Então existem $\alpha, \beta \in \bar{\mathbb{Q}}$ tais que*

$$e_n = 1 + q^n - \alpha^n - \beta^n$$

Mais ainda, para todo n podemos obter e_n a partir de e_1.
Prova: Seja ϕ_1 o q-ésimo morfismo de Frobenius em E. Portanto temos que

$$\phi_n = \phi_1^n$$

é o q^n-ésimo morfismo de Frobenius. Sabemos que

$$e_n = \#E(\mathbb{F}_{q^n}) = \deg([1] - \phi_1^n) = 1 - \mathrm{Tr}(\phi_1^n) + \deg\phi_1^n = 1 - \mathrm{Tr}(\phi_1^n) + q^n$$

Sejam $\alpha, \beta \in \bar{\mathbb{Q}}$ as raízes de $c_{\phi_1}(\mathrm{T})$. Aplicando o lema anterior a ϕ_1 obtemos

$$e_n = 1 + q^n - \alpha^n - \beta^n$$

Observemos que

$$\alpha^n + \beta^n = 1 + q^n - e_n \qquad \text{e} \qquad e_n = (\alpha^n - 1)(\beta^n - 1)$$

pois $q^n = \deg \phi_1^n = \alpha^n \beta^n$. Assim

$$\begin{aligned} e_n &= 1 + q^n - (\alpha^n + \beta^n) \\ (\text{ por } 4.1) &= 1 + q^n - ((\alpha+\beta)(\alpha^{m-1} + \beta^{m-1}) - \alpha\beta(\alpha^{m-2} + \beta^{m-2})) \\ &= 1 + q^n - ((1 + q - e_1)(1 + q^{m-1} - e_{m-1}) - q(1 + p^{m-2} - e_{m-2})). \end{aligned}$$

Como

$$\begin{aligned} e_2 &= (\alpha^2 - 1)(\beta^2 - 1) \\ &= (\alpha - 1)(\beta - 1)(\alpha + 1)(\beta + 1) \\ &= e_1(\alpha\beta + \alpha + \beta + 1) \\ &= e_1(q + 1 + q - e_1 + 1) \\ &= e_1(2(q+1) - e_1) \\ &= -e_1^2 + 2(q+1)e_1. \end{aligned}$$

logo, por indução, temos que e_m é uma função polinomial de grau m em e_1 a coeficientes inteiros. □

Infelizmente este resultado não proporciona uma maneira efetiva para o cálculo de e_n a partir de e_1. Se observarmos atentamente o caso $n = 2$ vemos que para obter e_n é necessário usar algumas substituições e vários cálculos algébricos. Vejamos como tornar efetivo o cálculo de e_n.

No espiríto dos resultados anteriores podemos definir

Definição 4.1 *A* função zeta da curva elíptica $E/\mathbb{F}_q$ *é a série de potências*

$$Z(E/\mathbb{F}_q; T) = \exp(\sum_{n=1}^{\infty} \frac{e_n T^n}{n})$$

Note que se conhecermos $Z(E/\mathbb{F}_q; T)$ então podemos recuperar seus coeficientes, e_n/n, na série pela fórmula

$$\frac{e_n}{n} = \frac{1}{n!} \frac{d^n}{dT^n} \log Z(E/\mathbb{F}_q; T) \Big|_{T=0}$$

O cálculo de e_n torna-se efetivo devido ao próximo teorema

Teorema 4.2.7 *Seja $\mathbb{F}_q$ um corpo com q elementos e $E/\mathbb{F}_q$ uma curva elíptica. Então existe um $a \in \mathbb{Z}$ tal que*

$$Z(E/\mathbb{F}_q;T) = \frac{1-aT+qT^2}{(1-T)(1-qT)}.$$

Além disso

$$Z(E/\mathbb{F}_q;\frac{1}{qT}) = Z(E/\mathbb{F}_q;T)$$

e

$$1-aT+qT^2 = (1-\alpha T)(1-\beta T),\ \textit{com}\ |\alpha| = |\beta| = \sqrt{q}.$$

Prova: Seja α e β como no teorema anterior. Portanto

$$\begin{aligned}
\log Z(E/\mathbb{F}_q;T) &= \sum_{n=1}^{\infty} \frac{e_n T^n}{n} \\
&= \sum_{n=1}^{\infty} \frac{(1+q^n-\alpha^n+\beta^n)T^n}{n} \\
&= \sum_{n=1}^{\infty} \frac{T^n}{n} + \sum_{n=1}^{\infty} \frac{(qT)^n}{n} + -\sum_{n=1}^{\infty} \frac{(\alpha T)^n}{n} - \sum_{n=1}^{\infty} \frac{(\beta T^n)}{n} \\
&= -\log(1-T) + \log(1-\alpha T) + \log(1-\beta T) - \log(1-qT) \\
&= \log \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}
\end{aligned}$$

logo

$$Z(E/\mathbb{F}_q;T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}.$$

Como $c_\phi(r) \geq 0$, $\forall r \in \mathbb{Q}$, temos que $\alpha = \bar{\beta}$ e logo $p = \alpha\beta = |\alpha|^2$. Daí

$$Z(E/\mathbb{F}_q;T) = \frac{1-\mathrm{Tr}(\phi)T+qT^2}{(1-T)(1-qT)}.$$

As demais afirmações são obtidas facilmente. □

Portanto o algoritmo para o cálculo de e_n é bastante simples e sua implementação no **Maple** é a seguinte

```
> a:=?;
> p:=?;
> n:=2:
> der:=ln((1-a*T+p*T^2)/((1-T)*(1-p*T))):
> for x from 1 to n do:
> der:=diff(der, T);
> end do:
> eval(der,T=0);
```

onde as interrogações representam números naturais apropriados.

Exemplo 4.1 *A cota de Hasse não pode ser melhorada* - Considere a curva dada pela equação de Weierstrass

$$E : y^2 + y = x^3$$

Ela será uma curva elíptica definida sobre $\mathbb{F}_{2^n}$, se em $\mathbb{F}_{2^n}$ tivermos $\Delta \neq 0$. Um cálculo simples nos mostra que $\Delta = -3^3$ e portanto E é uma curva elíptica definida sobre $\mathbb{F}_{2^n}$, para todo n. É fácil ver que

$$E(\mathbb{F}_2) = \{O, (0,0), (0,1)\}$$

e daí $e_1 = 3$. Portanto

$$\begin{aligned} e_2 &= (\alpha^2 - 1)(\beta^2 - 1) \\ &= (\alpha - 1)(\beta - 1)(\alpha + 1)(\beta + 1) \\ &= e_1(\alpha\beta + \alpha + \beta + 1) \\ &= e_1(2 + 1 + 2 - e_1 + 1) \\ &= 9 \end{aligned}$$

Logo

$$|\#E(\mathbb{F}_{2^2}) - 1 - 2^2| = |e_2 - 5| = 4 = 2 \cdot 2 = 2\sqrt{2^2}$$

mostrando-nos que a estimativa obtida não pode ser melhorada.

Exemplo 4.2 $E_{(n)} : y^2 = x^3 - n^2 x$.

Como $\Delta_n = (2n)^6$, $E_{(n)}$ será uma curva elíptica em $\mathbb{F}_p$, se $p \nmid 2n$. Suponhamos, para este exemplo, que $p \equiv 3 \mod 4$.

Notemos que $-\bar{x} = \overline{p-x}$ e que $f(x) = x(x^2 - n^2)$ é uma função ímpar. Observemos também que

$$E_{(n)}(\mathbb{Z}/p\mathbb{Z}) = \{O\} \cup \{(0,0)\} \cup \{(x, \pm\sqrt{f(x)}) \mid f(x) \text{ é um quadrado em } \mathbb{Z}/p\mathbb{Z}\}$$

e portanto

$$\#E_{(n)}(\mathbb{Z}/p\mathbb{Z}) = 2 \cdot \#\{x \mid f(x) \text{ é um quadrado em } \mathbb{Z}/p\mathbb{Z}\} + 2$$

Usando o símbolo de Legendre calculamos

$$\left(\begin{array}{c} f(-x) \\ p \end{array}\right) = \left(\begin{array}{c} -f(x) \\ p \end{array}\right) = \left(\begin{array}{c} -1 \\ p \end{array}\right) \cdot \left(\begin{array}{c} f(x) \\ p \end{array}\right) = -1 \cdot \left(\begin{array}{c} f(x) \\ p \end{array}\right)$$

já que $p \equiv 3 \mod 4$. Ou seja, $f(x)$ é um quadrado (em $\mathbb{Z}/p\mathbb{Z}$) se, e só se, $f(-x)$ não for um quadrado. Este fato e uma análise da próxima tabela nos diz que

$$\#\{x \mid f(x) \text{ é um quadrado em } \mathbb{Z}/p\mathbb{Z}\} = \frac{p-1}{2}$$

e portanto

$$\#E_{(n)}(\mathbb{Z}/p\mathbb{Z}) = 2 \cdot \frac{p-1}{2} + 2 = p + 1$$

x	$-x$
1	$p-1$
2	$p-2$
$\vdots$	$\vdots$
$\frac{p-1}{2} - 1$	$p - (\frac{p-1}{2} - 1) = \frac{p-1}{2} + 2$
$\frac{p-1}{2}$	$p - \frac{p-1}{2} = \frac{p-1}{2} + 1$

Capítulo 5

Teorema de Mordell

5.1 Teoria das Alturas

Faremos agora a demonstração de um dos resultados mais importantes sobre curvas elípticas: aquele que garante a finitude dos geradores de uma curva elíptica sobre os racionais.

Este teorema (e não uma conjectura) foi proposto por Poincaré [1901] em *Sur les Propriétes Arithmétiques des Courbes Algébriques* onde ele definiu o posto de uma curva elíptica sobre os racionais. Em 1922, na procura pela prova da finitude de soluções inteiras de um certo tipo de equação diofantina, Mordell finalmente demonstrou este teorema, que hoje recebe seu nome, no artigo *On the rational solutions of the indeterminate equations of the third and fourth degree*. Anos depois, A. Weil, em sua tese, generalizou bastante o resultado de Mordell, e o que hoje é chamado de Mordell-Weil trata na realidade da finitude de geradores de uma variedade abeliana sobre um corpo de números k. Segundo Cassels [CASSELS2], Mordell era totalmente contrário ao uso deste nome, chegando a "insistir freqüentemente (em público e em particular) que o que ele havia provado deveria ser chamado teorema de Mordell e que tudo o mais deveria ser chamado de Teorema de Weil".

A demonstração que se segue utiliza uma caracterização dos grupos abelianos A finitamente gerados a partir de uma função $|\ | : A \to \mathbb{R}$, chamada de *norma*, que satisfaz:
(i)$|P| \geq 0$, para todo P;
(ii) O conjunto $\{P \in A \mid |P| \leq c\}$ é finito para toda constante c;

(iii) $|[m]P| = |m||P|$, para todo $m \in \mathbb{Z}$ e todo $P \in A$;
(iv) $|P + Q| \leq |P| + |Q|$, $\forall P, Q \in A$.

Um exemplo de norma em um grupo abeliano finito A seria a norma trivial ou nula $|\ |_0$, definida por $|P|_0 = 0$, $\forall P \in A$.

Vejamos que vantagens imediatas uma função norma num grupo abeliano nos traz:

Teorema 5.1.1 *Seja A um grupo abeliano dotado de uma função norma. Então:*
(a) Um ponto $P \in A$ é de torção se, e somente se, $|P| = 0$.
(b) O subgrupo de torção de A é finito.
Prova: (a) Se existir um $m \in \mathbb{Z}\backslash\{0\}$ tal que $[m]P = 0$ então

$$0 = |[m]P| = |m||P|$$

Donde $|P| = 0$.

A recíproca obtem-se ao considerarmos o conjunto

$$\{[m]P \mid m \in \mathbb{Z}\}$$

Se $|P| = 0$, então $|[m]P| = 0$, para todo inteiro m, implicando assim que o conjunto acima é finito pelo axioma (ii).

(b) Basta aplicarmos o item (a) e o axioma (ii). □

Entretanto o resultado mais importante a respeito de uma norma num grupo abeliano é o seguinte:

Teorema 5.1.2 (Teorema da Descida) *Um grupo abeliano A é finitamente gerado se, e somente se, existe um inteiro $m \geq 2$ tal que A/mA é finito e o grupo A possui uma função norma.*
Prova: Suponhamos que $\{x_1, ..., x_n\}$ sejam geradores de A. Logo, para qualquer inteiro $m \geq 2$, A/mA é gerado por $\{\bar{x_1}, ..., \bar{x_n}\}$. Observe ainda que se para $a_i \in \mathbb{Z}$ tivermos $a_i \equiv r_i \mod m$ então $a_i\bar{x}_i = r_i\bar{x}_i$.

Seja $\bar{x} \in A/mA$. Então, para alguns $a_i \in \mathbb{Z}$

$$\bar{x} = a_1\overline{x_1} + ... + a_n\overline{x_n} = r_1\overline{x_1} + ... + r_n\overline{x_n}$$

pertencendo assim a um conjunto finito.

Pelo Teorema fundamental sobre grupos abelianos segue que

$$A \cong A_{tor} \times \mathbb{Z}^r$$

No entanto, $\mathbb{Z}^r$ possui uma norma herdada de $\mathbb{R}^r$: a restrição a $\mathbb{Z}^r$ da norma euclidiana. Como A_{tor} é finito, nele consideraremos a norma nula. Donde

$$|(P_1, P_2)| = |P_1|_0 + |P_2|$$

é a norma de um ponto $(P_1, P_2) \in A$.

Suponhamos que $A/mA = \{\bar{a_1}, ..., \bar{a_r}\}$, $r \in \mathbb{N}^*$, para algum inteiro $m \geq 2$. Suponhamos ainda que A possui uma função norma $|\ |$. Mostraremos que A é gerado pelo conjunto finito

$$G = \{P \in A \mid |P| \leq c_0\}$$

onde $c_0 = \text{máx}\{|a_1|, ..., |a_r|\}$.

Seja $x_0 \in A$. Se $x_0 \in G$ nada há para demonstrar. Caso $|x_0| > c_0$ tomemos a imagem de x_0 em A/mA, obtendo desta forma um representante a_{i_0} para x_0. Isto significa que para algum $x_1 \in A$ temos $x_0 = a_{i_0} + mx_1$. Portanto, pela desigualdade triangular temos

$$\begin{aligned} m|x_1| &= |x_0 - a_{i_0}| \\ &\leq |x_0| + |a_{i_0}| \\ &\leq |x_0| + c_0 \\ &< 2|x_0| \\ |x_1| &< \frac{2}{m}|x_0| \\ |x_1| &< |x_0| \end{aligned}$$

pois assumimos que $m \geq 2$.

Se $x_1 \in G$ então $x_0 = a_{i_0} + mx_1$ já está no subgrupo gerado por G. Caso contrário, pelo raciocínio acima, encontraremos um x_2 tal que

$$x_1 = a_{i_1} + mx_2, \qquad |x_2| < |x_1| \qquad \text{e} \qquad x_0 = a_{i_0} + ma_{i_1} + m^2x_2.$$

Continuando assim encontraremos uma seqüência de pontos $x_0, x_1, x_2, ...$ satisfazendo

$$|x_0| > |x_1| > |x_2| > ...$$

e tal que no r-ésimo passo temos

$$x_0 = a_{i_0} + ma_{i_1} + m^2 a_{i_2} + ... + m^{r-1} a_{i_{r-1}} + m^r x_r$$

com $a_{i_j} \in G$. No entanto esta seqüência não pode continuar indefinidamente, pois em A todo conjunto de pontos de norma limitada é finito, forçando que x_0 seja uma combinação linear de pontos em G. □

Este teorema recebe este nome, porque o argumento é bastante similar a um outro argumento utilizado por Fermat, que ele costumava chamar de *descente infinie*: a "descida ao infinito", herdeira imediata do Princípio da Boa Ordenação.

Nosso objetivo agora é construir uma função norma em $E = E(\mathbb{Q})$ e depois mostrar que $E/2E$ é finito. A asserção "$E/2E$ é finito" é normalmente conhecida pelo nome de *Teorema de Mordell fraco* justamente por implicar o teorema de Mordell de uma maneira quase imediata.

Antes façamos algumas reduções.

Como char($\mathbb{Q}$)= 0, teremos que a equação de Weierstrass poderá ser tomada da forma:

$$Y^2 = F(X)$$

com

$$F(X) = X^3 + aX + b, \qquad a, b \in \mathbb{Q} \qquad \text{e} \qquad 4a^3 + 27b^2 \neq 0$$

e onde esta última expressão garante que o polinômio $F(X)$ tem três raízes distintas.

Suponhamos que $a = \dfrac{r_a}{s_a}$ e $b = \dfrac{r_b}{s_b}$, com $r_a, s_a, r_b, s_b \in \mathbb{Z}, s_a, s_b \neq 0$. Fazendo a mudança $Y \to u^2 Y'$ e $Y \to u^3 Y'$ onde $u = s_a s_b$ temos que a equação de Weierstrass manterá a mesma forma $Y'^2 = X'^3 + a'X' + b'$, onde, entretanto, $a' = u^4 a$ e $b' = u^6 b$ serão números inteiros.

Seja $P = (x, y) \in E$. Como $x, y \in \mathbb{Q}$, podemos escrevê-los da seguinte forma:

$$x = \frac{p}{q},\ \text{mdc}(p, q) = 1 \text{ e } y = \frac{r}{s},\ \text{mdc}(r, s) = 1$$

P é solução de $Y^2 = X^3 + aX + b$ $(a, b \in \mathbb{Z})$, donde:

$$\begin{aligned}(\frac{r}{s})^2 &= (\frac{p}{q})^3 + a\frac{p}{q} + b \\ q^3r^2 &= s^2p^3 + as^2q^2p + bq^3s^2 \\ q^3r^2 &= s^2(p^3 + aq^2p + bq^3)\end{aligned}$$

Assim concluímos que

$$s^2 \mid q^3r^2 \Longrightarrow \text{ (pois mdc(r,s)=1) } s^2 \mid q^3$$

Também da última igualdade acima podemos deduzir, de uma maneira um pouco menos evidente, que

$$q^3 \mid s^2, \text{ já que } \text{mdc}(p, q) = 1$$

Ou seja $q^3 = \pm s^2$ e pela fatoração única nos inteiros deve existir $t \in \mathbb{Z}$ tal que

$$q = t^2 \text{ e } s = t^3$$

Além disso temos que $\text{mdc}(p, t^2) = \text{mdc}(r, t^3) = 1$.

É a partir da noção de altura que construíremos uma norma em E. Uma função altura é uma função que deve de alguma forma mostrar o quanto é complicado o ponto sob a ótica da teoria dos números, além de se comportar bem com relação a lei de grupo da curva elíptica. Para ilustrar esta preocupação começaremos definindo a altura de um número racional.

Seja $x = \dfrac{p}{q}$ um número racional irredutível. Definiremos a altura de x como sendo

$$H(x) = H(\frac{p}{q}) = \text{máx}\{|p|, |q|\}$$

"Por que não tomar a altura de um número racional como sendo o seu módulo?" seria uma pergunta muito natural. Observemos que 1 e $\dfrac{999999999}{1000000000}$ possuem módulos muito próximos, embora, para a teoria dos números, o segundo seja um número muito mais complicado que o primeiro. Além disso, essa função altura, ao

contrário do módulo, se comporta da maneira que se deseja para conjuntos de pontos cuja altura é limitada por uma constante; quero dizer que

$$\{x \in \mathbb{Q} \mid H(x) \leq c\}$$

é finito para qualquer constante c, pois existe um número finito de inteiros com módulo menor que c.

Seja agora $P = (x_0 : ... : x_n) \in \mathbb{P}^n_{\mathbb{Q}}$, um ponto no espaço projetivo de dimensão n sobre $\mathbb{Q}$. Podemos então definir a função $H : \mathbb{P}^n_{\mathbb{Q}} \to \mathbb{Q}$ da seguinte forma

$$H(x_0 : ... : x_n) = \prod_{2 \leq p: \text{ primo } \leq \infty} \text{máx}\{|x_0|_p, ..., |x_n|_p\}$$

onde o produto é feito sobre todos os primos p e $|\ |_p$ indica, como nas seções anteriores, a norma p-ádica em $\mathbb{Q}$ enquanto que $|\ |_\infty = |\ |$. Esta funcão está bem definida pois

Lema 5.1.3

$$\prod_{2 \leq p \leq \infty} |\lambda|_p = 1, \quad \forall \lambda \in \mathbb{Q}^*$$

Prova: Dado $\lambda \in \mathbb{Q}^*$ podemos sempre escrevê-lo como

$$\lambda = \pm \prod_{2 \leq p < \infty} p^{\alpha_p}$$

e $\alpha_p \in \mathbb{Z}$. E daí

$$|\lambda|_p = p^{-\alpha_p} \Longrightarrow \prod_{2 \leq p < \infty} |\lambda|_p = \prod_{2 \leq p < \infty} p^{-\alpha_p} = |\lambda|_\infty^{-1}$$

e portanto

$$\prod_{2 \leq p \leq \infty} |\lambda|_p = |\lambda|_\infty \prod_{2 \leq p < \infty} |\lambda|_p = |\lambda|_\infty |\lambda|_\infty^{-1} = 1$$

□

Portanto para $\lambda P = (\lambda x_0 : ... : \lambda x_n), \quad \lambda \in \mathbb{Q}^*$ temos

$$\begin{aligned} H(\lambda P) &= \prod_{2\leq p\leq\infty} \text{máx}\{|\lambda x_i|_p\} \\ &= \prod_{2\leq p\leq\infty} |\lambda|_p \,\text{máx}\{|x_i|_p\} \\ &= \prod_{2\leq p\leq\infty} |\lambda|_p \prod_{2\leq p\leq\infty} \text{máx}\{|x_i|_p\} \\ &= \prod_{2\leq p\leq\infty} \text{máx}\{|x_i|_p\} = H(P) \end{aligned}$$

e H está bem definida.

Um fato que merece uma certa atenção é que a altura de um número racional x, segundo esta definição, coincide com a altura do ponto $P_x = (1 : x) \in \mathbb{P}^1_{\mathbb{Q}}$. De fato, suponhamos que $x = \dfrac{m}{n}$ é uma fração irredutível e que a fatoração em primos é $m = p_1^{a_1}...p_r^{a_r}$ e $n = q_1^{b_1}...q_s^{b_s}$ onde $a_i, b_j \in \mathbb{N}^*$. Daí, como $\text{mdc}(p_i, q_j) = 1$, $\forall i, j$, temos

$$|x|_{p_i} = p_i^{-a_1} < 1 \qquad \text{e} \qquad |x|_{q_j} = q_j^{b_j} > 1$$

e

$$H(1 : x) = \text{máx}\{1, |x|_\infty\} \prod_{\substack{p\geq 2 \\ p:\text{primo}}} \text{máx}\{1, |x|_p\} = \text{máx}\{1, |x|_\infty\} \cdot n$$

Como $m \geq n \iff \text{máx}\{1, |x|_\infty\} = \dfrac{m}{n}$ e $n \geq m \iff \text{máx}\{1, |x|_\infty\} = 1$ então

$$H(1 : x) = n \cdot \text{máx}\{1, |x|_\infty\} = \text{máx}\{|m|, |n|\} = H(x).$$

Além disso, o conjunto $\{P \in \mathbb{P}^n_{\mathbb{Q}} \mid H(P) \leq c\}$ é finito para toda constante real c.

Definamos, ainda, uma função $H : E \to \mathbb{Z}$ por

$$H(P) = \begin{cases} H(x), & \text{se } P = (x, y) \neq O \\ 1, & \text{para } P = O \end{cases}$$

Observemos que ao calcularmos $H(P)$ só olhamos o que acontece com a coordenada x. Fazemos isto justamente porque ao limitarmos $H(x) = H(P)$ estaremos de certa forma limitando automaticamente $H(y)$. De fato, ao escrevermos $P = (\dfrac{p}{t^2}, \dfrac{r}{t^3})$

temos que $|p| \leq H(P)$ e $|t|^2 \leq H(P)$. Usando o fato de P satisfazer a equação da curva obtemos

$$r^2 = p^3 + at^4p + bt^6$$

que em módulo nos dá

$$\begin{aligned} |r|^2 &\leq |p|^3 + |a||t^4p| + |b||t^6| \\ &\leq (1 + |a| + |b|)H(P)^3 \\ |r| &\leq (\sqrt{1 + |a| + |b|})H(P)^{3/2} = \kappa H(P)^{3/2} \end{aligned}$$

Veremos que $H(P)$ se "comporta de uma maneira multiplicativa", isto é, $H(P+Q)$ está de alguma forma relacionado com $H(P)H(Q)$. Por razões notacionais, seria mais agradável que a função altura tivesse um "comportamento aditivo". Por isso, é conveniente que definamos a altura (logarítmica) de um ponto P como sendo

$$h(P) = \begin{cases} \log H(x(P)), & \text{se } P \neq O \\ 0, & \text{para } P = O \end{cases}$$

E pelas mesmas razões definimos a altura (logarítmica) de um ponto P no espaço projetivo $\mathbb{P}^n(\mathbb{Q})$ como sendo

$$h(P) = \log(H(P))$$

A primeira propriedade importante satisfeita pela altura em espaços projetivos é a que relaciona a altura de um ponto $P \in \mathbb{P}^n$ com a altura de sua imagem por um morfismo entre espaços projetivos $F : \mathbb{P}^n \to \mathbb{P}^m$. Aqui, faz-se necessário rever a definição do que seria um morfismo.

Definição 5.1 *Um morfismo de grau d entre espaços projetivos sobre os racionais é uma aplicação*

$$\begin{array}{rcl} F : \mathbb{P}^n & \longrightarrow & \mathbb{P}^m \\ P & \longmapsto & F(P) = (f_0(P), ..., f_m(P)) \end{array}$$

onde $f_0, ..., f_m \in \mathbb{Q}[X_0, ..., X_n]$ *são polinômios homogêneos de grau d sem raízes comuns em* $\bar{\mathbb{Q}}$ *que não seja a trivial.*

Recordemos também que a condição imposta acima sobre os polinômios $f_0, ..., f_m$ é equivalente a dizer que existe um s tal que $< f_0, ..., f_m > \supset < X_0, ..., X_n >^{s+d}$,

como afirma o "Nullstellensatz homogêneo". Isto implica que existem polinômios homogêneos $g_{ij} \in \mathbb{Q}[X_0, ..., X_n]$ de grau s tais que

$$\sum_{0 \leq j \leq m} g_{ij}(\underline{X}) f_j(\underline{X}) = X_i^{s+d}$$

o que, limpando os denominadores, nos leva a concluir que

$$\sum_{0 \leq j \leq m} g_{ij}(\underline{X}) f_j(\underline{X}) = b X_i^{s+d}$$

com os $g_{ij} \in \mathbb{Z}[X_0, ..., X_n]$ e b um número inteiro.

Teorema 5.1.4 *Seja $F : \mathbb{P}^n \to \mathbb{P}^m$ um morfismo de grau d. Então existem constantes c_1 e c_2, dependentes unicamente de F, tais que*

$$c_1 H(P)^d \leq H(F(P)) \leq c_2 H(P)^d$$

para todo ponto $P \in \mathbb{P}^n$.
Prova: Sejam $f_0, ..., f_n \in \mathbb{Z}[X_0, ..., X_n]$ polinômios homogêneos de grau d que definem F.

Para obtermos a estimativa superior, façamos o seguinte para todo $i \in \{0, ..., n\}$ e todo primo q:

$$|f_i(P)|_q = |\sum_{(I)} a_{i_{(I)}} x^{(I)}|_q \leq \sum_{(I)} |a_{i_{(I)}}|_q |x^{(I)}|_q \leq \sum_{(I)} |a_{i_{(I)}}|_q (\text{máx}\{|x_i|_q\})^d$$

Observe que com este cálculo extraímos um fato de caráter geral: dado um polinômio homogêneo $f \in \mathbb{Q}[\underline{X}]$ de grau d sempre existe uma constante $c(f)$ tal que $|f(P)|_q \leq c(f)(\text{máx}\{|x_i|_q\})^d$.

Donde concluímos que

$$\text{máx}\{|f_i(P)|_q\} \leq \text{máx}\{\sum_{(I)} |a_{i_{(I)}}|_q (\text{máx}\{|x_i|_q\})^d\} \leq \text{máx}\{\sum_{(I)} |a_{i_{(I)}}|_q\} (\text{máx}\{|x_i|_q\})^d$$

e portanto

$$H(F(P)) = \prod_r \text{máx}\{|f_i(P)|_q\} \leq \prod_r c_2 (\text{máx}\{|x_i|_q\})^d = c_2 H(P)^d$$

para $c_2 = \text{máx}\{\sum_{(I)} |a_{i_{(I)}}|_q\}$.

Já a estimativa inferior é um pouco mais complicada e requer as observações feitas acima sobre o Nullstellensatz.

Das equações

$$\sum_j g_{ij}(P) f_j(P) = b x_i^{s+d}$$

podemos deduzir que os divisores comuns dos f_j's devem dividir b, pois $\text{mdc}(x_0, ..., x_n) = 1$.

Usando ainda as equações e inequação acima, além do fato geral sobre formas e altura que destacamos anteriormente chegamos a seguinte estimativa

$$\begin{aligned} |bx_i^{s+d}|_q = |\sum_j g_{ij}(P) f_j(P)|_q &\leq \sum_j |g_{ij}|_q |f_j(P)|_q \\ &\leq \text{máx}\{|x_i|_q\}^s \sum_j c(g_{ij}) |f_j(P)|_q \\ &\leq \text{máx}\{|x_i|_q\}^s \,\text{máx}\{c(g_{ij})\} \sum_j |f_j(P)|_q \\ &\leq \kappa \,\text{máx}\{|x_i|_q\}^s \,\text{máx}\{|f_j(P)|_q\} \end{aligned}$$

onde $\kappa = (m+1)\,\text{máx}\{c_j(g_{ij})\}$.

Tomando o máximo sobre todos os i da desigualdade acima concluímos que

$$(\text{máx}\{|x_i|_q\})^{s+d} \leq \frac{\kappa}{|b|_q} (\text{máx}\{|x_i|_q\})^s \,\text{máx}\{|f_j(P)|_q\}$$

Tomando o produtório em q desta desigualdade e efetuando alguns cancelamentos, chegamos a expressão desejada para alguma constante $c_1 > 0$:

$$c_1 H(P)^d \leq H(F(P))$$

□

No que se segue, o próximo lema será bastante útil:

Lema 5.1.5 *Sejam $P = (p_0 : p_1)$ e $Q = (q_0 : q_1)$ pontos na reta projetiva racional. Considere o ponto $R = (p_0q_0 : p_0q_1 + p_1q_0 : p_1q_1) \in \mathbb{P}^2$. Então*

$$\frac{1}{2}H(P)H(Q) \leq H(R) \leq 2H(P)H(Q)$$

Prova: Seja r um primo, então

$$\begin{aligned} |p_0q_0|_r &\leq 2\,\text{máx}\{|p_i|_r\}\,\text{máx}\{|q_i|_r\} \\ |p_0q_1 + p_1q_0|_r &\leq |p_0q_1|_r + |p_1q_0|_r \leq 2\,\text{máx}\{|p_i|_r\}\,\text{máx}\{|q_i|_r\} \\ |p_1q_1|_r &\leq H(P)H(Q) \leq 2\,\text{máx}\{|p_i|_r\}\,\text{máx}\{|q_i|_r\} \end{aligned}$$

Portanto

$$\text{máx}\{|p_0q_0|_r, |p_0q_1 + p_1q_0|_r, |p_1q_1|_r\} \leq 2\,\text{máx}\{|p_i|_r\}\,\text{máx}\{|q_i|_r\}$$

e daí

$$H(R) = \prod_r \text{máx}\{|p_0q_0|_r, |p_0q_1+p_1q_0|_r, |p_1q_1|_r\} \leq \prod_r 2\,\text{máx}\{|p_i|_r\}\,\text{máx}\{|q_i|_r\} = 2H(P)H(Q)$$

Para cada primo fixo r, consideremos os seguintes casos

- $\text{máx}\{|p_i|_r\} = |p_0|_r$ e $\text{máx}\{|q_i|_r\} = |q_0|_r$
  Assim temos

$$\begin{aligned} \frac{1}{2}\,\text{máx}\{|p_i|_r\}\,\text{máx}\{|q_i|_r\} &\leq \text{máx}\{|p_i|_r\}\,\text{máx}\{|q_i|_r\} = |p_0q_0|_r \\ &\leq \text{máx}\{|p_0q_0|_r, |p_0q_1 + p_1q_0|_r, |p_1q_1|_r\} \end{aligned}$$

- $\text{máx}\{|p_i|_r\} = |p_1|_r$ e $\text{máx}\{|q_i|_r\} = |q_1|_r$
  De maneira análoga a anterior mostra-se que

$$\frac{1}{2}\,\text{máx}\{|p_i|_r\}\,\text{máx}\{|q_i|_r\} \leq \text{máx}\{|p_0q_0|_r, |p_0q_1 + p_1q_0|_r, |p_1q_1|_r\}$$

- $\text{máx}\{|p_i|_r\} = |p_0|_r$ e $\text{máx}\{|q_i|_r\} = |q_1|_r$
  Suponhamos que $\frac{1}{2}\,\text{máx}\{|p_i|_r\} \leq |p_1|_r$ ou $\frac{1}{2}\,\text{máx}\{|q_i|_r\} \leq |q_0|_r$. No primeiro caso temos

  $$\frac{1}{2}|p_0q_1|_r = \frac{1}{2}\,\text{máx}\{|p_i|_r\}\,\text{máx}\{|q_i|_r\} \leq |p_1q_1| \leq \text{máx}\{|p_0q_0|_r, |p_0q_1+p_1q_0|_r, |p_1q_1|_r\}$$

No segundo

$$\frac{1}{2}|p_0q_1|_r = \frac{1}{2}\,\text{máx}\{|q_i|_r\}\,\text{máx}\{|p_i|_r\} \leq |p_0q_0|_r \leq \text{máx}\{|p_0q_0|_r, |p_0q_1+p_1q_0|_r, |p_1q_1|_r\}$$

Do contrário teríamos então que $|p_1|_r \leq \frac{1}{2}\,\text{máx}\{|p_i|_r\}$ e $|q_0|_r \leq \frac{1}{2}\,\text{máx}\{|q_i|_r\}$. Donde

$$|p_1q_0|_r \leq \frac{1}{4}\,\text{máx}\{|p_i|_r\}\,\text{máx}\{|q_i|_r\}$$

Por outro lado, podemos usar esta desigualdade acima para obtermos

$$\begin{array}{rcl}
\text{máx}\{|p_i|_r\}\,\text{máx}\{|q_i|_r\} = |p_0q_1|_r & \leq & |p_0q_1 + p_1q_0|_r + |p_1q_0|_r \\
& \Downarrow & \\
\text{máx}\{|p_i|_r\}\,\text{máx}\{|q_i|_r\} - |p_1q_0|_r & \leq & |p_0q_1 + p_1q_0|_r \leq M(R) \\
& \Downarrow & \\
\text{máx}\{|p_i|_r\}\,\text{máx}\{|q_i|_r\} - \frac{1}{4}\,\text{máx}\{|p_i|_r\}\,\text{máx}\{|q_i|_r\} & \leq & M(R) \\
& \Downarrow & \\
\frac{1}{2}\,\text{máx}\{|p_i|_r\}\,\text{máx}\{|q_i|_r\} \leq \frac{3}{4}\,\text{máx}\{|p_i|_r\}\,\text{máx}\{|q_i|_r\} & \leq & M(R)
\end{array}$$

com $M(R) = \text{máx}\{|p_0q_0|_r, |p_0q_1 + p_1q_0|_r, |p_1q_1|_r\}$

- $\text{máx}\{|p_i|_r\} = |p_1|_r$ e $\text{máx}\{|q_i|_r\} = |q_0|_r$
  Segue, por simetria, do caso anterior que

$$\frac{1}{2}\,\text{máx}\{|p_i|_r\}\,\text{máx}\{|q_i|_r\} \leq \text{máx}\{|p_0q_0|_r, |p_0q_1 + p_1q_0|_r, |p_1q_1|_r\}$$

Em qualquer dos casos anteriores temos, para todo primo r

$$\frac{1}{2}\,\text{máx}\{|p_i|_r\}\,\text{máx}\{|q_i|_r\} \leq \text{máx}\{|p_0q_0|_r, |p_0q_1+p_1q_0|_r, |p_1q_1|_r\} \leq \text{máx}\{|p_i|_r\}\,\text{máx}\{|q_i|_r\}$$

o que, tomando o produtório em r, torna-se

$$\frac{1}{2}H(P)H(Q) \leq H(R) \leq 2H(P)H(Q)$$

□

Teorema 5.1.6 *Seja $E(\mathbb{Q})$ uma curva elíptica. Então existem constantes c_1 e c_2, que dependem apenas de E, tais que para todo ponto P e Q em E temos*

$$c_1 H(P)^2 H(Q)^2 \leq H(P+Q)H(P-Q) \leq c_2 H(P)^2 H(Q)^2$$

Prova: Sejam $P = (x_1, y_1)$, $Q = (x_2, y_2)$, $P + Q = (x_3, y_3)$ e $P - Q = (x_4, y_4)$. Observemos que

$$H(P) = H(x_1) = H(1 : x_1)$$

onde o segundo H indica a altura de um número racional e o terceiro a altura do ponto $(1 : x_1) \in \mathbb{P}^1(\mathbb{Q})$.

A idéia da demonstração é mostrar que existe um morfismo $F : \mathbb{P}^2 \to \mathbb{P}^2$ de grau 2 que leva o ponto $R_1 = (1 : x_1 + x_2 : x_1 x_2)$ no ponto $R_2 = F(R_1) = (1 : x_3 + x_4 : x_3 x_4)$. Se isso ocorrer então, como afirma o teorema anterior, existirão constantes c_1' e c_2' tais que

$$c_1' H(1 : x_1 + x_2 : x_1 x_2)^2 \leq H(1 : x_3 + x_4 : x_3 x_4) \leq c_2' H(1 : x_1 + x_2 : x_1 x_2)^2 \qquad (*)$$

Notemos que os pontos $R_1 = (1 : x_1 + x_2 : x_1 x_2)$ e $R_2 = (1 : x_3 + x_4 : x_3 x_4)$ satisfazem as condições do lema anterior para os pontos $(1 : x_1)$ e $(1 : x_2)$, no caso de R_1; $(1 : x_3)$ e $(1 : x_4)$, no caso de R_2. Usando a primeira desigualdade acima e o lema anterior temos

$$\frac{1}{4} c_1' H(1 : x_1)^2 H(1 : x_2)^2 \leq H(1 : x_3 + x_4 : x_3 x_4) \leq 2H(1 : x_3)H(1 : x_4)$$

E portanto, pela observação feita inicialmente, obtemos

$$c_1 H(P)^2 H(Q)^2 \leq H(P+Q)H(P-Q)$$

com $c_1 = \dfrac{1}{8} c_1'$.

Da mesma forma, usando a segunda desigualdade em $(*)$ e a desigualdade dada pelo lema anterior temos

$$H(1 : x_3 + x_4 : x_3 x_4) \leq c_2' H(1 : x_1 + x_2 : x_1 x_2)^2 \leq 4c_2' H(1 : x_1)^2 H(1 : x_2)^2$$

e daí

$$\frac{1}{2} H(1 : x_3)H(1 : x_4) \leq 4c_2' H(1 : x_1)^2 H(1 : x_2)^2$$

que, para $c_2 = 8c_2'$, equivale a

$$H(P+Q)H(P-Q) \leq c_2 H(P)^2 H(Q)^2$$

Para encontrarmos este morfismo F, partiremos do ponto $R_2 = (1 : x_3 + x_4 : x_3x_4)$. Lembremos que $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ e $(x_4, y_4) = (x_1, y_1) + (x_2, -y_2)$. Assim ao usarmos a fórmula para a adição de pontos distintos P e Q obtemos

$$\begin{aligned} x_3 &= (\frac{y_2 - y_1}{x_2 - x_1})^2 - (x_1 + x_2) \\ x_4 &= (\frac{y_2 + y_1}{x_2 - x_1})^2 - (x_1 + x_2) \end{aligned}$$

donde

$$\begin{gathered} (1 : x_3 + x_4 : x_3x_4) \\ = \\ ((x_2 - x_4)^4 : [(y_2 - y_1)^2 + (y_2 + y_1)^2](x_2 - x_1)^2 - 2(x_2 + x_1)(x_2 - x_1)^4 : \\ [(y_2 - y_1)^2 - (x_2 + x_1)(x_2 - x_1)^2][(y_2 + y_1)^2 - (x_2 + x_1)(x_2 - x_1)^2]) \\ = \\ ((x_2 - x_1)^4 : 2(x_2 - x_1)^2(y_1^2 + y_2^2 - (x_1 + x_2)(x_1 - x_2)^2) : \\ (y_1^2 - y_2^2)^2 + (x_1 - x_2)^4(x_1 + x_2)^2 - 2(x_1 - x_2)^2(x_1 + x_2)(y_1^2 + y_2^2)) \\ = \\ ((x_1 - x_2)^2 : 2(x_1x_2^2 + x_1^2x_2 + a(x_1 + x_2) + 2b) : (x_1x_2 - a)^2 - 4b(x_1 + x_2)) \end{gathered}$$

Note que esta última expressão está definida para quaisquer pontos P e Q em E, sejam eles distintos ou não. O fato importante agora é que está última expressão pode ser escrita da seguinte forma

$$\begin{gathered} (1 : x_3 + x_4 : x_3x_4) \\ = \\ ((x_1 - x_2)^2 : 2(x_1x_2^2 + x_1^2x_2 + a(x_1 + x_2) + 2b) : (x_1x_2 - a)^2 - 4b(x_1 + x_2)) \\ = \\ (f_0(1 : x_1 + x_2 : x_1x_2) : f_1(1 : x_1 + x_2 : x_1x_2) : f_2(1 : x_1 + x_2 : x_1x_2)) \end{gathered}$$

onde $f_0(X, Y, Z) = Y^2 - 4XZ$, $f_1(X, Y, Z) = 2YZ + 2aXY + 4bX^2$ e $f_2(X, Y, Z) = (Z - aX)^2 - 4bXY$ são formas de grau 2.

Suponhamos que $f_0(X,Y,Z)$, $f_1(X,Y,Z)$ e $f_2(X,Y,Z)$ possuam um zero não trivial em comum $(t:u:v)$. Neste caso temos que $t \neq 0$ senão teríamos

$$\begin{aligned} f_0(0:u:v) &= u^2 = 0 \Longrightarrow u = 0 \\ f_1(0:u:v) &= 2uv = 0 \\ f_2(0:u:v) &= v^2 = 0 \Longrightarrow v = 0 \end{aligned}$$

Logo faz sentido tomarmos a quantia $x = \dfrac{u}{2t}$. Portanto

$$u^2 = 4tv \Longrightarrow \frac{u^2}{4t^2} = \frac{4tv}{4t^2} \Longrightarrow x^2 = \frac{v}{t}$$

Dividindo as equações

$$\begin{aligned} 2uv + 2atu + 4bt^2 &= 0 \\ (v - at)^2 - 4btu &= 0 \end{aligned}$$

por t^2 temos

$$\begin{aligned} \frac{2u}{t}\frac{v}{t} + 2a\frac{u}{t} + 4b &= 0 \\ (\frac{v}{t} - a)^2 - 4b\frac{u}{t} &= 0 \end{aligned}$$

isto é

$$\begin{aligned} 4(x^3 + ax + b) &= 0 \\ (x^2 - a)^2 - 8bx &= 0 \end{aligned}$$

Destas equações acima deduzimos

$$0 = x^4 - 2ax^2 + a^2 - 8bx = (3x^2 + a)^2 - 8x(x^3 + ax + b) = (3x^2 + a)^2$$

contrariando o fato de que $F(X) = X^3 + aX + b$ possui três raízes complexas distintas. Logo $f_0(X,Y,Z)$, $f_1(X,Y,Z)$ e $f_2(X,Y,Z)$ não possuem zeros em comum. □

A desigualdade obtida dá origem a uma constante c tal que

$$|h(P+Q) + h(P-Q) - 2h(P) - 2h(Q)| \leq c$$

e isto, para $P = Q$, é

$$|h([2]P) - 4h(P)| \leq c$$

E daí, para inteiros $n \geq m \geq 0$, encontramos as seguintes desigualdades

$$\begin{aligned} |h([2^n]P) - 4h([2^{n-1}]P)| &\leq c \\ |4h([2^{n-1}]P) - 4^2h([2^{n-2}]P)| &\leq c \\ |4^2h([2^{n-2}]P) - 4^3h([2^{n-3}]P)| &\leq c \\ &\ldots \\ |4^{n-m-1}h([2^{m+1}]P) - 4^{n-m}h([2^m]P)| &\leq c \end{aligned}$$

cuja soma é

$$|h([2^n]P) - 4^{n-m}h([2^m]P)| \leq (n-m)c \leq nc$$

que, ao dividirmos por 4^n, torna-se

$$|\frac{h([2^n]P)}{4^n} - \frac{h([2^m]P)}{4^m}| = |\frac{h([2^n]P) - 4^{n-m}h([2^m]P)}{4^n}| \leq \frac{nc}{4^n}$$

Mostramos assim que a seqüência $\{\frac{h([2^n]P)}{4^n}\}$ é de Cauchy, pois $\frac{nc}{4^n} \longrightarrow 0$; logo converge. Portanto, faz sentido definir uma função $\hat{h} : E \to \mathbb{R}$ por

$$\hat{h}(P) = \lim_{n \to +\infty} \frac{h([2^n]P)}{4^n}$$

Esta recebe o nome de *altura canônica* e satisfaz:

Teorema 5.1.7 *(a) ("Lei do Paralelogramo")* $\hat{h}(P+Q)+\hat{h}(P-Q) = 2h(\hat{Q})+2\hat{h}(Q)$*;*

(b) Para todo inteiro m*,* $\hat{h}([m]P) = m^2\hat{h}(P)$*;*

(c) $\hat{h}(P)$ *é uma forma quadrática positiva em* E*;*

(d) Existe uma constante c *tal que* $|\hat{h}(P) - h(P)| \leq c$*;*

(e) $\{P \in E \mid \hat{h}(P) \leq \kappa\}$ *é um conjunto finito para toda constante* κ*.*

Prova: (a) Segue da definição de $\hat{h}(P)$ e da desigualdade

$$|h(P+Q) + h(P-Q) - 2h(P) - 2h(Q)| \leq c.$$

(b) Temos que

$$\begin{aligned}\hat{h}([m+1]P) &= \hat{h}([m]P+P)\\ &= 2\hat{h}([m]P)+2\hat{h}(P)-\hat{h}([m-1]P)\\ &= 2m^2\hat{h}(P)+2\hat{h}(P)-(m-1)^2\hat{h}(P)\\ &= (2m^2+2-(m-1)^2)\hat{h}(P)\\ &= (m+1)^2\hat{h}(P)\end{aligned}$$

Assim o resultado segue por indução.

(c) De $h(-P)=h(P)$ concluímos que $\hat{h}(-P)=\hat{h}(P)$.

Mostremos que $B(P,Q)=\dfrac{1}{2}(\hat{h}(P+Q)-\hat{h}(P)-\hat{h}(Q))$ é uma forma bilinear simétrica que satisfaz $\hat{h}(P)=B(P,P)$.

Temos claramente que $\hat{h}(P)=B(P,P)$ e que $B(P,Q)=B(Q,P)$. Logo só nos resta mostrar que

$$B(P+R,Q)=B(P,Q)+B(R,Q)$$

Se usarmos o fato de que $\hat{h}(-P)=\hat{h}(P)$ e a lei do paralelogramo obtemos as igualdades

$$\begin{aligned}\hat{h}(P+R+Q)+\hat{h}(P+R-Q)-2\hat{h}(P+R)-2\hat{h}(Q)=0\\ -\hat{h}(P-R+Q)-\hat{h}(P+R-Q)+2\hat{h}+2\hat{h}(R-Q)=0\\ \hat{h}(P-R+Q)+\hat{h}(P+R+Q)-2\hat{h}(P+Q)-2\hat{h}(R)=0\\ -2\hat{h}(R+Q)-2\hat{h}(R-Q)+4\hat{h}(R)+4\hat{h}(Q)=0\end{aligned}$$

cuja soma é

$$2\hat{h}(P+Q+R)-2\hat{h}(P+R)-2\hat{h}(P+Q)-2\hat{h}(Q+R)+2\hat{h}(P)+2\hat{h}(Q)+2\hat{h}(R)=0$$

isto é

$$\begin{aligned}B(P+R,Q) &= \frac{1}{2}(\hat{h}(P+Q+R)-\hat{h}(P+Q)-\hat{h}(R))\\ &= \frac{1}{2}(\hat{h}(P+Q)-\hat{h}(P)-\hat{h}(Q)+\hat{h}(R+Q)-\hat{h}(R)-\hat{h}(Q)\\ &= B(P,Q)+B(R,Q)\end{aligned}$$

(d) Como vimos acima, encontramos uma constante c tal que, para inteiros $n \geq m \geq 0$, tenhamos

$$|\frac{h([2^n]P)}{4^n} - \frac{h([2^m]P)}{4^m}| \leq \frac{nc}{4^n} \leq c$$

Fazendo $m = 0$ e $n \to +\infty$ obtemos

$$|\hat{h}(P) - h(P)| \leq c$$

(e) Suponhamos que $P \in E$ seja tal que $\hat{h}(P) \leq \kappa$, para alguma constante κ. Assim, por (d)

$$|h(P)| = |h(P) - \hat{h}(P) + \hat{h}(P)| \leq |\hat{h}(P) - h(P)| + |\hat{h}(P)| \leq c + \kappa$$

isto quer dizer que P pertence ao conjunto

$$\{P \in E \mid |h(P)| \leq c + \kappa\}$$

que é um conjunto finito. □

Como resultado imediato obtemos

Corolário 5.1.8 $|P| := \sqrt{\hat{h}(P)}$ *é uma norma em* E.
Prova: Trivial. □

5.2 O Teorema de Mordell Fraco

Nesta seção mostraremos um resultado do qual o Teorema de Mordell decorre imediatamente, que é chamado usualmente de Mordell Fraco. O enunciado do teorema é bastante simples:

Teorema 5.2.1 (Mordell Fraco) *Seja* $E(\mathbb{Q})$ *uma curva elíptica. Então* $E/2E$ *é finito.*

Antes de demonstrá-lo façamos algumas considerações.

Seja $\mathbb{Q}[\theta] = \dfrac{\mathbb{Q}[T]}{F(T)}$, onde $\theta = T \mod F(T)$. Suponhamos, para fixar idéia, que $F(X)$ possua dois fatores irredutíveis $p_1(X)$ e $p_2(X)$. Então utilizando o Teorema do Resto Chinês e o homomorfismo sobrejetivo

$$\begin{array}{rcl} \mathbb{Q}[X] & \longrightarrow & \dfrac{\mathbb{Q}[X]}{p_1(X)} \times \dfrac{\mathbb{Q}[X]}{p_2(X)} \\ h(X) & \longmapsto & (h(X) \mod p_1(X), g(X) \mod p_2(X)) \end{array}$$

temos que $\mathbb{Q}[\theta]$ é a soma direta de tantos corpos quanto são seus fatores irredutíveis.

Caso $F(X)$ possua uma raíz $q \in \mathbb{Q}$ então teremos um isomorfismo ϕ entre $\mathbb{Q}[\theta]$ e $\dfrac{\mathbb{Q}[X]}{X-q} \times \dfrac{\mathbb{Q}[X]}{G(X)}$, onde $G(X) = X^2 + qX + q^2 + a$. Assim um elemento de $\mathbb{Q}[\theta]$ pode ser visto como um par do tipo $(h(X) \mod (X-q), h(X) \mod G(X))$.

Seja $\alpha \in \mathbb{Q}[\theta]$. Como podemos enxergar $\mathbb{Q}[\theta]$ como um $\mathbb{Q}$-espaço vetorial de dimensão 3, então a associação $\xi \longmapsto \alpha\xi$, para $\xi \in \mathbb{Q}[\theta]$, definirá um mapa linear α cujo determinante chamaremos da norma de α, representada por $\mathrm{Norm}(\alpha)$. Como $\alpha\beta = \alpha \circ \beta$ vemos que $\mathrm{Norm}(\alpha\beta) = \det(\alpha \circ \beta) = \mathrm{Norm}(\alpha)\,\mathrm{Norm}(\beta)$ e que α é invertível se, e só se, $\mathrm{Norm}(\alpha) \neq 0$.

Seja $x \in \mathbb{Q}$. Pondo $x - \theta = \tau$, então:

$$\begin{array}{rcl} \tau(1) & = & (x-\theta).1 = x.1 - 1.\theta \\ \tau(\theta) & = & (x-\theta).\theta = x.\theta - \theta^2 \\ \tau(\theta^2) & = & (x-\theta).\theta^2 = x.\theta^2 - 1.\theta^3 \\ & = & x\theta^2 - (-a\theta - b) = b.1 + a\theta + x\theta^2 \end{array}$$

donde concluímos

$$\mathrm{Norm}(\tau) = \begin{vmatrix} x & 0 & b \\ -1 & x & a \\ 0 & -1 & x \end{vmatrix} = x^3 + ax + b = F(x)$$

Caso $F(q) = 0$, para algum $q \in \mathbb{Q}$, notemos que o isomorfismo ϕ entre $\mathbb{Q}[\theta]$ e $\dfrac{\mathbb{Q}[X]}{X-q} \times \dfrac{\mathbb{Q}[X]}{G(X)}$ preserva a norma. De fato, uma base para $\dfrac{\mathbb{Q}[X]}{X-q} \times \dfrac{\mathbb{Q}[X]}{G(X)}$ seria

$$\{(1,0), (0,1), (0,\gamma)\}$$

onde $\gamma = X \mod G(X)$. Assim a norma de $(x-q, x-\gamma) = \phi(x-\theta)$ será exatamente $F(x)$, para $x \in \mathbb{Q}$, o que pode ser obtido fazendo-se um cálculo semelhante ao anterior. (OBS: A multiplicação aqui é feita componente a componente.)

A partir deste momento usaremos indiscriminadamente o isomorfismo entre $\mathbb{Q}[\theta]$ e $\frac{\mathbb{Q}[X]}{X-q} \times \frac{\mathbb{Q}[X]}{G(X)}$ para representar um elemento de $\mathbb{Q}[\theta]$. Por exemplo, consideraremos "iguais" os elementos $x-\theta$ e $(x-q, x-\gamma)$, caso $q \in \mathbb{Q}$ seja uma raíz de $F(X)$.

Denotemos por K^* ao grupo multiplicativo dos elementos invertíveis de $K = \mathbb{Q}[\theta]$. Então $(K^*)^2$ é claramente um subgrupo de K^*.

Desta forma $\frac{K^*}{(K^*)^2}$ é um grupo e representaremos seus elementos por $[\alpha]$, $\alpha \in K^*$.

Considere $\mathcal{M} \subset \frac{K^*}{(K^*)^2}$ consistindo dos elementos $[\alpha]$ para os quais $\text{Norm}(\alpha) \in (\mathbb{Q}^*)^2$. Não é difícil mostrar que $\mathcal{M}$ é um subgrupo de $\frac{K^*}{(K^*)^2}$.

Denotemos por μ o mapa $E \to \mathcal{M}$, definido da seguinte maneira:

- $\mu(O) = [1]$
- $\mu(P) = [x-\theta]$, quando $P = (x, y) \in E$, $y \neq 0$.
- Se $P = (q, 0) \in E$, então $F(q) = 0$. E daí, $\text{Norm}(q-\theta) = 0 \notin (\mathbb{Q}^*)^2$. Para contornar este problema escolhamos um elemento $\beta \in \mathbb{Q}^*$ de modo que $h(\theta) = (\beta, q-\gamma)$ tenha norma em $(\mathbb{Q}^*)^2$.
  Aqui também faremos $\gamma = X \mod G(X)$ com $G(X) = X^2 + qX + q^2 + a$, o que implica que $-\gamma^2 = q\gamma + q^2 + a$.
  Suponhamos que, para algum $t \in \mathbb{Q}^*$, tenhamos $t^2 = \text{Norm}((\beta, q-\gamma))$. Calculemos $\text{Norm}((\beta, q-\gamma))$

$$\begin{aligned}
(\beta, q-\gamma).(1,0) &= (\beta, 0) = \beta(1,0) \\
(\beta, q-\gamma).(0,1) &= (0, q-\gamma) \\
&= q(0,1) + (-1)(0,\gamma) \\
(\beta, q-\gamma).(0,\gamma) &= (0, q\gamma - \gamma^2) \\
&= (0, q\gamma + q\gamma + q^2 + a) \\
&= (q^2+a)(0,1) + 2q(0,\gamma)
\end{aligned}$$

Portanto

$$t^2 = \text{Norm}(h(\theta)) = \begin{vmatrix} \beta & 0 & 0 \\ 0 & q & q^2+a \\ 0 & -1 & 2q \end{vmatrix} = \beta(2q^2+q^2+a) = \beta(2q^2+a) = \beta F'(q)$$

Donde $\beta = \dfrac{t^2}{F'(q)}$, já que $F'(q) \neq 0$, pois F possui três raízes distintas. Assim se $h'(\theta) = (\beta', q-\gamma)$ é tal que $\text{Norm}(h'(\theta)) = s^2$ então teremos que

$$\begin{aligned} \mu(P) &= [(\beta', q-\gamma)] \\ &= [(\beta', q-\gamma)(\frac{t}{s}, 1)^2] \\ &= [(\frac{s^2}{F'(q)}, q-\gamma)(\frac{t^2}{s^2}, 1)] \\ &= [(\frac{s^2}{F'(q)}\frac{t^2}{s^2}, q-\gamma)] \\ &= [(\beta, q-\gamma)] \end{aligned}$$

Mostramos, assim, que $\mu(P) = [h(\theta)]$ estará bem definido.

Lema 5.2.2 *O mapa μ é um homomorfismo de grupos.*
Prova: Sejam $P_i = (a_i, b_i) \in E$, $i \in \{1, 2, 3\}$, pontos sobre uma mesma reta

$$Y = lX + m \qquad l, m \in \mathbb{Q}$$

Então

$$P_1 + P_2 + P_3 = O$$

Daí $(a_3, -b_3) = -P_3 = P_1 + P_2$ e $\mu(P_3) = \mu(-P_3) = [a_3 - \theta]$.

Portanto, a interseção da reta com a curva elíptica E será dada por

$$F(X) - (lX + m)^2 = (X - a_1)(X - a_2)(X - a_3)$$

Este polinômio em $\mathbb{Q}[\theta]$ é visto como

$$-(l\theta + m)^2 = (\theta - a_1)(\theta - a_2)(\theta - a_3)$$

equivalentemente

$$(a_3 - \theta)(l\theta + m)^2 = (a_1 - \theta)(a_2 - \theta)(a_3 - \theta)^2$$

Caso $b_i \neq 0, \forall i$, temos que

$$\begin{aligned}
\mu(P_1)\mu(P_2) &= [(a_1 - \theta)][(a_2 - \theta)] \\
&= [(a_1 - \theta)][(a_2 - \theta)][(a_3 - \theta)^2] \\
&= [(a_3 - \theta)(l\theta + m)^2] \\
&= \mu(-P_3) \\
&= \mu(P_1 + P_2)
\end{aligned}$$

Suponhamos que $P_1 = (a_1, 0)$ e $P_2 = (a_2, b_2)$, com $b_2 \neq 0$. Seja $P_3 = (a_3, b_3)$ o terceiro ponto de interseção de E com a reta ligando P_1 a P_2. Mais uma vez $P_1 + P_2 = -P_3$. Além disso, se esta reta tem equação $Y = lX + m$ então

$$F(X) - (lX + m)^2 = (X - a_1)G(X) - (lX + m)^2 = (X - a_1)(X - a_2)(X - a_3) \quad (5.1)$$

E esta equação módulo $G(X)$ é igual a

$$(l\gamma + m)^2 = (a_1 - \gamma)(a_2 - \gamma)(a_3 - \gamma) \quad (5.2)$$

$$(a_3 - \gamma)(l\gamma + m)^2 = (a_1 - \gamma)(a_2 - \gamma)(a_3 - \gamma)^2 \quad (5.3)$$

Além disso a equação (5.1) dá origem a seguinte relação

$$(X - a_1) \mid (lX + m)^2 \Longrightarrow (lX + m)^2 = \alpha(X - a_1)^2$$

ou seja

$$G(X) - \alpha^2(X - a_1) = (X - a_2)(X - a_3)$$

$$F'(a_1) = G(a_1) = (a_2 - a_1)(a_3 - a_1)$$

Logo

$$\begin{aligned}
\mu(P_1)\mu(P_2) &= [(\frac{t^2}{F'(a_1)}, a_1-\gamma)][(a_2-a_1, a_2-\gamma)] \\
&= [(\frac{t^2}{(a_2-a_1)(a_3-a_1)}(a_2-a_1), (a_2-\gamma)(a_1-\gamma))] \\
&= [(\frac{t^2}{(a_3-a_1)}, (a_2-\gamma)(a_1-\gamma))] \\
&= [(\frac{t^2}{(a_3-a_1)}, (a_2-\gamma)(a_1-\gamma))(a_3-a_1, a_3-a_1)^2] \\
&= [(\frac{t^2}{(a_3-a_1)}, (a_2-\gamma)(a_1-\gamma))((a_3-a_1)^2, (a_3-a_1)^2)] \\
&= [(t^2(a_3-a_1), (a_2-\gamma)(a_1-\gamma)(a_3-a_1)^2)] \\
&= [(t^2(a_3-a_1), (a_3-\gamma)(l\gamma+m)^2)] \\
&= [(a_3-a_1, a_3-\gamma)(t^2, (l\gamma+m)^2)] \\
&= [(a_3-a_1, a_3-\gamma)] \\
&= \mu(-P_3)
\end{aligned}$$

Resta-nos mostrar que para os pontos $P_i = (a_i, 0)$, $i \in \{1, 2, 3\}$, também vale

$$\mu(P_1)\mu(P_2) = \mu(-P_3) = \mu(P_3)$$

Note que

$$F(X) = (X-a_1)(X-a_2)(X-a_3)$$

Donde

$$\mathbb{Q}[\theta] \cong \frac{\mathbb{Q}[X]}{X-a_1} \times \frac{\mathbb{Q}[X]}{X-a_2} \times \frac{\mathbb{Q}[X]}{X-a_3}$$

Portanto

$$\begin{aligned}
a_1-\theta &= (0, a_1-a_2, a_1-a_3) \\
a_2-\theta &= (a_2-a_1, 0, a_2-a_3) \\
a_3-\theta &= (a_3-a_1, a_3-a_2, 0)
\end{aligned}$$

e

$$\text{Norm}(a_i-\theta) = 0, \quad \forall i$$

Mais uma vez para contornarmos este problema devemos escolher $\beta_1, \beta_2, \beta_3 \in \mathbb{Q}^*$ de modo que

$$\begin{aligned}
&\text{Norm}((\beta_1, a_1 - a_2, a_1 - a_3)) \in (\mathbb{Q}^*)^2 \\
&\text{Norm}((a_2 - a_1, \beta_2, a_2 - a_3)) \in (\mathbb{Q}^*)^2 \\
&\text{Norm}((a_3 - a_1, a_3 - a_2, \beta_3)) \in (\mathbb{Q}^*)^2
\end{aligned}$$

Impondo esta condição veremos que β_i deverá ser do tipo

$$\beta_i = \frac{t_i^2}{\prod\limits_{1 \leq j \neq i \leq 3} (a_j - a_i)}, \quad \forall i$$

para alguns $t_i \in \mathbb{Q}^*$.

Daí podemos concluir que

$$\begin{aligned}
\mu(P_1) &= [(\frac{t_1^2}{(a_2 - a_1)(a_3 - a_1)}, a_1 - a_2, a_1 - a_3)] \\
\mu(P_2) &= [(a_2 - a_1, \frac{t_2^2}{(a_2 - a_1)(a_2 - a_3)}, a_2 - a_3)] \\
\mu(P_3) &= [(a_3 - a_1, a_3 - a_2, \frac{t_3^2}{(a_3 - a_1)(a_3 - a_2)})]
\end{aligned}$$

Façamos os seguintes cálculos

$$\begin{aligned}
\mu(P_1)\mu(P_2) &= [(\frac{t_1^2}{(a_3 - a_1)}, \frac{t_2^2}{(a_3 - a_2)}, (a_1 - a_3)(a_2 - a_3))] \\
&= [(\frac{t_1^2}{(a_3 - a_1)}, \frac{t_2^2}{(a_3 - a_2)}, (a_3 - a_1)(a_3 - a_2))\mathbf{v^2}] \\
&= [(a_3 - a_1, a_3 - a_2, \frac{t_3^2}{(a_3 - a_1)(a_3 - a_2)})] \\
&= \mu(P_3)
\end{aligned}$$

onde $\mathbf{v} = (\frac{a_3 - a_1}{t_1}, \frac{a_3 - a_2}{t_2}, \frac{t_3}{(a_3 - a_1)(a_3 - a_2)})$. □

Lema 5.2.3 *$Ker(\mu) = 2E$.*
Prova: Seja $P \in E$. Então

$$\mu(2P) = (\mu(P))^2 = [1]$$

mostrando, portanto, que $2E \subset \mathrm{Ker}(\mu)$.

Seja agora $P = (x, \pm y) \in E$ tal que $\mu(P) = [1]$.

Se $y \neq 0$, então $\bar{1} = \mu(P) = [x - \theta]$, implicando que

$$x - \theta = (p_2\theta^2 + p_1\theta + p_0)^2$$

para alguns $p_j \in \mathbb{Q}$.

Se $y = 0$, então, por tudo que vimos anteriormente, temos que

$$x - \theta = (0, x - \gamma)$$

Fazendo $(0, x - \gamma) = (0, m_1 + m_2\gamma)^2$ encontramos um sistema de equações em m_1 e m_2 que possui solução, mostrando que $x - \theta$ é um quadrado em $\mathbb{Q}[\theta]$.

De qualquer forma sempre conseguimos encontrar $p_0, p_1, p_2 \in \mathbb{Q}$ tais que

$$x - \theta = (p_2\theta^2 + p_1\theta + p_0)^2$$

com $p_2 \neq 0$, pois caso contrário θ satisfaria o polinômio

$$p(X) = (p_1X + p_0)^2 + X - x$$

que tem grau 2.

Se impusermos que seja nulo o coeficiente de θ^2 em

$$(s_1\theta + s_0)(p_2\theta^2 + p_1\theta + p_0) = (s_1p_1 + s_0p_2)\theta^2 + (s_1p_0 + s_0p_1 - s_1p_2a)\theta + (s_0p_0 - s_1p_2b)$$

obtemos $s_0, s_1, r_0, r_1 \in \mathbb{Q}$, com $s_1p_1 = -s_0p_2$, de modo que

$$(s_1\theta + s_0)(p_2\theta^2 + p_1\theta + p_0) = r_1\theta + r_0$$

$s_1 = 0$ e $s_0 \neq 0$ implica que $p_2 = 0$. Logo podemos supor que $s_1 = -1$.

Então a nossa equação se torna

$$\begin{aligned}(s_0-\theta)(p_2\theta^2+p_1\theta+p_0) &= r_1\theta+r_0\\ &\Downarrow\\ (s_0-\theta)^2(x-\theta)^2 &= (r_1\theta+r_0)^2\end{aligned}$$

Como esta é uma equação em $\mathbb{Q}[\theta]=\dfrac{\mathbb{Q}[X]}{F(X)}$ podemos encontrar um $A(X)\in\mathbb{Q}[X]$ tal que

$$(r_1X+r_0)^2-(s_0-X)^2(x-X)^2=A(X)F(X)$$

Desenvolvendo ambos os membros desta igualdade, vê-se imediatamente que a única situação possível de ocorrer é $A(X)\equiv 1$.

Portanto a reta

$$Y=r_1X+r_0$$

intercepta $Y^2=F(X)$ nos pontos $P=(x,\pm y)$ e $Q=(s_0,r_1s_0+r_0)$, este último com multiplicidade 2.

Logo $P+Q+Q=0$, donde

$$P=2(-Q)$$

□

E finalmente temos a demonstração do Mordell Fraco:
Prova: O lema anterior nos diz que é suficiente mostrar que a imagem de $\mu: E\to\mathcal{M}$ é finita.

Para tanto, basta considerarmos apenas os pontos P de E tais que $P=(x,y)$ e $y\neq 0$, já que o complementar deste conjunto em E é finito. Podemos ainda supor que E tem infinitos elementos.

Como vimos anteriormente, este ponto P pode ser escrito da seguinte forma

$$(\frac{r}{t^2},\frac{p}{t^3}) \qquad \text{onde } r,p,t\in\mathbb{Z} \text{ e } \mathrm{mdc}(p,t^2)=\mathrm{mdc}(r,t^3)=1$$

Suponhamos agora que $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in \bar{\mathbb{Q}}$ são as três raízes distintas de $F(X)$. Logo

$$\begin{aligned} y^2 &= (x-\varepsilon_1)(x-\varepsilon_2)(x-\varepsilon_3) \\ \frac{r^2}{t^6} &= (\frac{p}{t^2}-\varepsilon_1)(\frac{p}{t^2}-\varepsilon_2)(\frac{p}{t^2}-\varepsilon_3) \\ r^2 &= (p-\varepsilon_1 t^2)(p-\varepsilon_2 t^2)(p-\varepsilon_3 t^2) \end{aligned}$$

Seja $K = \mathbb{Q}(\varepsilon_1, \varepsilon_2, \varepsilon_3)$. K é um corpo de números algébricos, logo, $\Im_K$, anel de inteiros de K, possui fatoração única de ideais. Sendo assim:

$$< r^2 >=< (p-\varepsilon_1 t^2) >< (p-\varepsilon_2 t^2) >< (p-\varepsilon_3 t^2) >$$

já que $p - \varepsilon_j t^2 \in \Im_K$.

Pela unicidade da fatoração, tem-se que um fator primo de $< p-\varepsilon_j t^2 >$ que não aparece em nenhum dos $< p-\varepsilon_i t^2 >$, para $i \neq j$, deve aparecer elevado ao quadrado na fatoração de $< r >^2$.

Vejamos o que acontece, por exemplo, com $< p-\varepsilon_j t^2, p-\varepsilon_j t^2 >$, um fator comum a $< p-\varepsilon_1 t^2 >$ e $< p-\varepsilon_2 t^2 >$:

$$\begin{aligned} < (\varepsilon_1-\varepsilon_2)t^2 >=< (p-\varepsilon_2 t^2)-(p-\varepsilon_1 t^2) > &\subset < p-\varepsilon_1 t^2, p-\varepsilon_2 t^2 > \\ < (\varepsilon_1-\varepsilon_2)p >=< \varepsilon_1(p-\varepsilon_2 t^2)-\varepsilon_2(p-\varepsilon_1 t^2) > &\subset < p-\varepsilon_1 t^2, p-\varepsilon_2 t^2 > \\ < (\varepsilon_1-\varepsilon_2)t^2, (\varepsilon_1-\varepsilon_2)p > &\subset < p-\varepsilon_1 t^2, p-\varepsilon_2 t^2 > \end{aligned}$$

Como $\text{mdc}(p, t^2) = 1$, existem $z_1, z_2 \in \mathbb{Z}$ tais que $z_1 p + z_2 t^2 = 1$. Multiplicando esta igualdade por $(\varepsilon_1 - \varepsilon_2)$ teremos que

$$< (\varepsilon_1-\varepsilon_2) >\subset < p-\varepsilon_1 t^2, p-\varepsilon_2 t^2 >$$

Portanto, pode-se concluir que

$$(*) \qquad < p-\varepsilon_j t^2 >= \Gamma_j(\Phi_j)^2$$

onde Γ_j é um fator de $< (\varepsilon_1-\varepsilon_2)(\varepsilon_1-\varepsilon_3)(\varepsilon_2-\varepsilon_3) >$ e portanto pertencerá a um conjunto de cardinalidade finita. Ademais, $\Gamma_1\Gamma_2\Gamma_3$ é um quadrado, pela fatoração única.

Observemos o que acontece com a igualdade $(*)$, quando a olhamos em $c\ell(K)$: o grupo de classes de ideais de K. Denotaremos por $[\wp]$ a classe do ideal $\wp$.

Como existe um número finito de Γ_j, fixado um deles, teremos que, para cada $< p - \varepsilon_j t^2 >$ dividido por este Γ_j, existirá um ideal $(\Phi_j)^2$, onde a igualdade $(*)$ poderá ser lida da forma

$$[1] = [\Gamma_j][\Phi_j]^2$$

Seja $[\Psi_j]$ a classe tal que $[\Phi_j][\Psi_j] = [1]$, isto é, $\Phi_j\Psi_j =< \delta_j >$. Assim

$$[\Gamma_j] = [\Gamma_j]([\Phi_j][\Psi_j])^2 = [\Gamma_j][\Phi_j]^2[\Psi_j]^2 = [\Psi_j]^2$$

Portanto existem um número finito de $u_j, v_j \in \Im_K$ tais que

$$< u_j > \Gamma_j =< v_j > \Psi_j^2$$

Daí

$$\begin{aligned} < u_j >< p - \varepsilon_j t^2 > &= < u_j > \Gamma_j \Phi_j^2 \\ &= < v_j > \Psi_j^2 \Phi_j^2 \\ &= < v_j > (\Psi_j \Phi_j)^2 \\ &= < v_j >< \delta_j^2 > \end{aligned}$$

Portanto

$$(p - \varepsilon_j t^2) = \nu_j \frac{v_j}{u_j} \delta_j^2$$

onde ν é uma unidade. Pela finitude dos geradores do grupo das unidades temos que $\eta_j = \nu_j \frac{v_j}{u_j}$ pertence a um conjunto finito. Logo

$$x - \varepsilon_j = \eta_j (\frac{\delta_j}{t})^2$$

Assim

$$x - \theta = \eta (\frac{\delta}{t})^2$$

com η num conjunto finito. Ou seja

$$\mu(P) = [x - \theta] = [\eta]$$

Mostrando o que queríamos mostrar: a finitude da imagem de μ. $\square$

5.3 O Teorema de Mordell

Os resultados anteriores permitem demonstrar

Teorema 5.3.1 (O Teorema de Mordell) *Seja $E/\mathbb{Q}$ uma curva elíptica. O grupo abeliano $E(\mathbb{Q})$ é finitamente gerado.*
Prova: O primeiro resultado deste capítulo (**5.1.2**, pg. 105) nos dá um critério para a finitude dos geradores de um grupo abeliano A: a finitude das classes de A/mA, para algum $m \geq 2$, e a existência de uma função norma em A. Na seção anterior mostramos que $E/2E$ é finito (**5.2.1**, pg. 121), enquanto que em (**5.1.8**, pg. 121) construímos uma função norma para E. □

Como já foi salientado algumas vezes, este resultado garante a existência de um natural r tal que:

$$E(\mathbb{Q}) = E(\mathbb{Q})_{tors} \times \mathbb{Z}^r$$

o número r é o *posto* de uma curva elíptica e é ainda hoje enigmático, apesar de existir ao seu respeito um conjunto de conjecturas numericamente plausíveis.

Como dissemos no princípio deste capítulo, A. Weil em 1928 generalizou enormemente o resultado de Mordell, estendendo-o para variedades abelianas sobre corpos de números. Uma *variedade abeliana sobre K* é um par (A, O) com A uma variedade completa sobre K dotada de uma estrutura de grupo onde as operações são morfismos e $O \in A(K)$ é um ponto K-racional de A. Uma curva elíptica, como mostramos, é uma variedade abeliana de dimensão 1.

Teorema 5.3.2 (Mordell-Weil) *Seja A uma variedade abeliana definida sobre um corpo de números K. Então o grupo $A(K)$ dos pontos K-racionais é finitamente gerado.*
Prova: [HINDRY-SILVERMAN], pg. 257. □

Para uma curva elíptica E sobre $K = k(C)$, um corpo de funções de uma curva, consegue-se demonstrar o teorema de Mordell fraco ($E(K)/2E(K)$ é finitamente gerado), consegue-se definir uma funcão altura que, em certos casos, permite aplicar o Teorema da descida e mostrar o Mordell para corpos de funções. Entretanto este

teorema não vale sempre devido ao fato de que dada uma curva C e seu corpo de finções $k(C)$, existem E/K e E_0/k, curvas elípticas, tais que

$$E_0 \hookrightarrow E$$

Se $k = \mathbb{C}$, por exemplo, temos que existe um retículo $\Lambda \subseteq \mathbb{C}$ tal que

$$E_0(\mathbb{C}) \simeq \frac{\mathbb{C}}{\Lambda}$$

e logo E/K não é finitamente gerado. Para todos os detalhes, recomendamos o capítulo 3 de [SILVERMAN2].

Exemplo 5.1 *A Cúbica de Fermat* - A cúbica de Fermat,

$$x^3 + y^3 = z^3 \tag{5.4}$$

é não singular, logo tem gênero 1. É portanto uma curva elíptica. Mostraremos que esta curva tem posto nulo.

Mostraremos na realidade que a equação (5.4) não possui soluções (x, y, z), com $xyz \neq 0$, no corpo $K = \mathbb{Q}[\omega]$, onde ω é uma raíz cúbica primitiva da unidade, isto é,

$$\omega^2 + \omega + 1 = 0.$$

Consideremos o anel de K-inteiros, $R = \mathbb{Z}[\omega]$. R satisfaz

Teorema 5.3.3 *(i)* $R = \{a + b\omega \mid a, b \in \mathbb{Z}\}$*;*
(ii) R *é um domínio de fatoração única;*
(iii) As unidades de R *são as potências de* ω*;*
(iv) Seja $\lambda = 1 - \omega$*. Então , para* $\alpha \in R$ *vale*

$$\alpha \equiv -1, 0 \text{ } ou \text{ } 1 \mod \lambda.$$

(v) Os primos de R *são os primos inteiros* q *tais que* $q \equiv -1 \mod 3$*; os números* $\pi \in R$ *cuja norma é* $N(\pi) = p$*,* $p \in \mathbb{Z}$ *primo satisfazendo* $p \equiv 1 \mod 3$*; e o número* $\lambda = 1 - \omega$
Prova: [ROSE], pg. 99. □

Notemos que

$$\lambda^2 = 1 - 2\omega + \omega^2 = 1 - 2\omega - 1 - \omega = -3\omega$$

e portanto

$$3 = -\lambda^2\omega^2.$$

Suponhamos que x, y, z seja uma solução para (5.4) com $xyz \neq 0$.

Já que (5.4) é homogênea podemos supor que $x, y, z \in R$, $\text{mdc}(x, y, z) = 1$, $\text{mdc}(x, y) = 1$, $\text{mdc}(x, z) = 1$ e $\text{mdc}(y, z) = 1$. Mostremos que $xyz \equiv 0 \mod \lambda$.

Seja $d = a + b\omega \in R$. Logo

$$d = a + b\omega = a + b(1 - \lambda) \Longrightarrow d \equiv a + b \mod \lambda.$$

Se $(a + b) \equiv 0 \mod 3$ então

$$d \equiv a + b \equiv 3k \equiv -k\lambda^2\omega^2 \equiv 0 \mod \lambda.$$

Assim para $d \not\equiv 0 \mod \lambda$ obteremos $a+b \equiv \pm 1 \mod 3$. Portanto se $xyz \not\equiv 0 \mod \lambda$ teremos

$$x, y, z \equiv \pm 1 \mod 3\lambda$$

e daí

$$x^3 + y^3 + z^3 \equiv \pm 1 \text{ ou } \pm 3 \mod 3\lambda.$$

De qualquer forma

$$x^3 + y^3 + z^3 \not\equiv 0 \mod 3\lambda$$

Uma contradição óbvia.

Assim, assumiremos que $z \equiv 0 \mod \lambda$ e daí

$$z = \eta'\lambda^n z'$$

onde η' é uma unidade, $n \geq 1$ é um inteiro e $\text{mdc}(z', \lambda) = 1$. Substituindo esta expressão em (5.4) conseguimos

$$x^3 + y^3 = \eta\lambda^{3n} z'^3$$

com η uma unidade, $\text{mdc}(z', \lambda) = 1$. E como $\text{mdc}(x, y) = 1$, segue que $\text{mdc}(x, y, \lambda) = 1$. De

$$0 \equiv x^3 + y^3 \equiv (x + y)((x + y)^2 - 3xy) \mod \lambda^3$$

obtemos

$$x + y \equiv 0 \mod \lambda \text{ e portanto } x = -y + t\lambda$$

Assim

$$x^3 + y^3 = -y^3 + 3y^2\lambda t - 3y\lambda^2 t^2 + \lambda^3 t^3 + y^3 = 3y^2\lambda t - 3y\lambda^2 t^2 + \lambda^3 t^3$$

Como $3 = -\lambda^2\omega^2$ temos que $x^3 + y^3 \mod \lambda^4$ será

$$\begin{aligned} x^3 + y^3 &\equiv \lambda^3 t^3 + \lambda^2\omega^2\lambda^2 t^2 y - \lambda^2\omega^2\lambda t y^2 \\ &\equiv \lambda^3 t(t^2 - \omega^2 y^2) \mod \lambda^4 \end{aligned}$$

Por (**5.3.3**, pg. 133) temos $t \equiv 0$ ou $\pm 1 \mod \lambda$. Se $t \equiv 0 \mod \lambda$ obtemos

$$x^3 + y^3 \equiv 0 \mod \lambda^4$$

Do contrário temos $t^2 = 1 + l_1\lambda$. Como $\text{mdc}(y, \lambda) = 1$ temos $y^2 = 1 + l_2\lambda$ e portanto

$$\begin{aligned} x^3 + y^3 &\equiv \lambda^3 t(t^2 - \omega^2 y^2) \\ &\equiv \lambda^3 t(1 + l_1\lambda - \omega^2(1 + l_2\lambda)) \\ &\equiv \lambda^3 t(1 - \omega^2) \\ &\equiv \lambda^3 t(1 - \omega)(1 + \omega) \\ &\equiv 0 \mod \lambda^3 \end{aligned}$$

Ou seja $x^3 + y^3 \equiv 0 \mod \lambda^3 \Longrightarrow x^3 + y^3 \equiv 0 \mod \lambda^4$. Mostraremos que a solução de

$$x^3 + y^3 = \eta\lambda^{3n} z'^3$$

implica a existência de x_0, y_0, z_0 tal que

$$x_0^3 + y_0^3 = \eta\lambda^3 z_0'^3$$

donde teremos

$$\begin{aligned} \eta\lambda^3 z_0'^3 = x_0^3 + y_0^3 &\equiv 0 \mod \lambda^4 \\ z' &\equiv 0 \mod \lambda \end{aligned}$$

contrariando o fato de termos $\text{mdc}(z', \lambda) = 1$. Logo não pode existir uma solução para (5.4) além daquelas satisfazendo $xyz = 0$.

Escrevamos

$$(*) \qquad (x+y)(x+\omega y)(x+\omega^2 y) = \eta\lambda^{3n} z'^3.$$

Notemos que

$$x + \omega y = x + y - \lambda y$$
$$x + \omega^2 = x + y + \lambda(-2+\lambda)y$$

logo λ divide todos os três fatores do primeiro membro de $(*)$. Uma potência de λ maior do que 1 deve dividir apenas um destes fatores, pois se, por exemplo, λ^2 dividisse $x+y$ e $x+\omega y$ teríamos

$$\lambda^2 g = \lambda^2 h - \lambda y$$

e logo λ deve dividir y, e, como vimos, isto não pode acontecer. Podemos então supor que

$$x + y = \eta_1 \lambda^{3n-2} z_1^3 \quad x + \omega y = \eta_2 \lambda z_1^3 \quad x + \omega^2 y = \eta_3 \lambda x_1^3$$

onde os η_i's são unidades, $\text{mdc}(x_1 y_1, \lambda) = 1$, $\text{mdc}(x_1, y_1, z_1) = 1)$, $x_1 y_1 z_1 = z' \neq 0$. Temos que

$$\begin{aligned} 0 &= (1+\omega+\omega^2)x + (1+\omega+\omega^2)y \\ &= \omega(x+y) + \omega^2(x+\omega y) + x + \omega^2 y \\ &= \omega\eta_1\lambda^{3n-2} z_1^3 + \omega^2\eta_2\lambda z_1^3 + \eta_3\lambda x_1^3 \end{aligned}$$

ou

$$x_1^3 + \zeta_1 y_1^3 = \zeta\lambda^{3(n-1)} z_1^3$$

com ζ_1 e ζ unidades. Supondo $n > 1$ temos

$$x_1^3 + \zeta_1 y_1^3 \equiv 0 \mod \lambda^3.$$

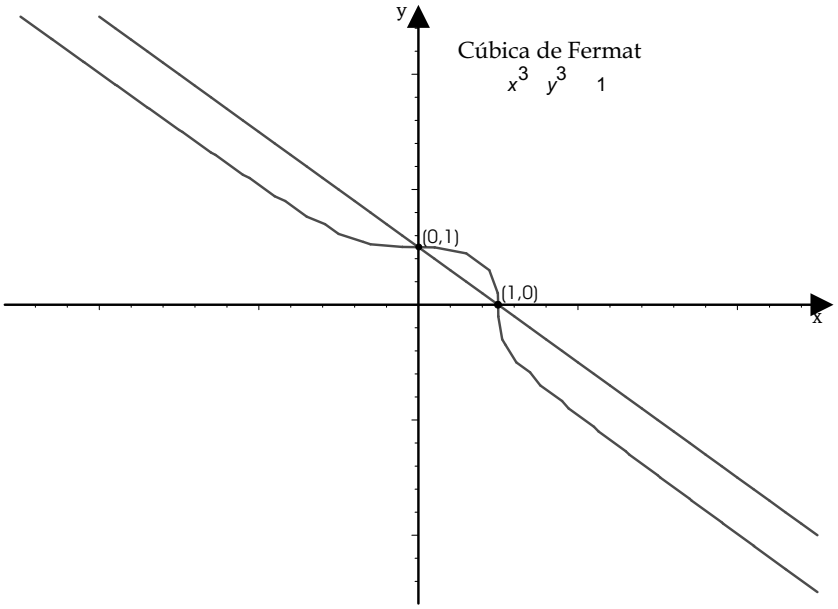
E, já que λ não divide $x_1 y_1$, temos

$$x_1^3 \equiv \pm 1 \mod \lambda^3 \qquad \text{e} \qquad y_1^3 \equiv \pm 1 \mod \lambda^3$$

e portanto

$$\zeta_1 \equiv \pm 1 \mod \lambda^3 \qquad \text{e} \qquad \zeta_1 = \pm 1$$

Assim mostramos que uma solução de $x^3 + y^3 = \eta\lambda^{3n} z'^3$ implica uma solução para $x_0^3 + y_0^3 = \zeta\lambda^{3(n-1)} z_0^3$, e pelo processo de descida, obtemos o resultado desejado.



Logo a cúbica de Fermat E é um exemplo de uma curva elíptica sobre $\mathbb{Q}$ que possui uma estrutura de grupo finito. No infinito ($z = 0$) temos o ponto $O = (-1 : 1 : 0)$, enquanto que os pontos afins desta cúbica claramente são $P = (1, 0)$ e $Q = (0, 1)$. A reta $x = 1$, $y = 1$ e $y = -x$ são tangentes inflexionais de P, Q e O, respectivamente. Portanto se tomarmos O como elemento neutro de nosso grupo, vemos que

$$P + Q = O.$$

Ademais, temos que $2P = Q$ e $2Q = P$ (lembre-se da definição geométrica da estrutura de grupo). Portanto

$$E(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}.$$

Exemplo 5.2 *Equação de Mordell* - A curva elíptica dada pela equação de Weierstrass

$$y^2 = x^3 - k$$

é chamada de *curva elíptica de Mordell*, por ter sido profundamente estudada por L.J. Mordell. Elas são os principais exemplos de curvas elípticas, cuja estrutura de grupo é a trivial, isto é, a curva não possui pontos afins racionais.

Podemos sempre supor que k é um inteiro livre de sexta potência, já que a transformação $x \to u^2x$ e $y \to u^3y$ leva esta curva em $u^6y^2 = u^6x^3 + k$. Os seguintes

resultados e exemplos encontram-se no livro de [MORDELL2], pg. 250:

Teorema 5.3.4 *A equação $y^2 = x^3+k$ não possui nenhuma solução racional quando as seguintes condições são satisfeitas:*

1. *k é negativo e livre de quadrados, $k \equiv 2, 3 \mod 4$ e $k \equiv 2, 4 \mod 9$;*
2. *O número de classes de ideais do corpo quadrático $\mathbb{Q}(\sqrt{k})$ não é divisível por 3.*
3. *Uma solução fundamental (u, t) de $Y^2 + 3kX^2 = 1$ satisfaz $u \not\equiv 0 \mod 3$.*

□

E os números $k = -5, -14, -34, -41$ satisfazem todas estas condições e daí, para $E : y^2 = x^3 - 5$

$$E(\mathbb{Q}) \simeq O.$$

Capítulo 6

Estrutura do grupo de Torção

6.1 O Teorema de Nagell-Lutz e o de Mazur

No capítulo anterior demonstramos que toda curva elíptica E definida sobre $\mathbb{Q}$ é tal que

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \times \mathbb{Z}^r$$

O posto r de uma curva elíptica é bastante difícil de determinar e, embora existam algoritmos que determinam limites inferiores e superiores para o posto, nenhum método efetivo é ainda conhecido. Este número é personagem de inúmeras conjecturas que desempenham um papel determinante no desenvolvimento da Teoria dos números.

Já a estrutura do subgrupo de torção de qualquer curva elíptica é bastante conhecida e possui uma maneira efetiva de determiná-la devida aos seguintes teoremas:

Teorema 6.1.1 (Nagell-Lutz) *Seja $E/\mathbb{Q}$ uma curva elíptica com equação de Weierstrass*

$$y^2 = x^3 + ax + b, \qquad a, b \in \mathbb{Z}$$

Suponha que $P \in E(\mathbb{Q})_{tors}$ é não nulo. Então

$$x(P), y(P) \in \mathbb{Z}$$

e

$$y(P) = 0 \ \ ([2]P = O) \qquad ou \qquad y(P)^2 | (4a^3 + 27b^2) = -\frac{\Delta}{16}$$

Prova: [CASSELS], pg. 50. □

Teorema 6.1.2 (Mazur) *Seja $E/\mathbb{Q}$ uma curva elíptica. Então o grupo de torção, $E(\mathbb{Q})_{tors}$, é um dos 15 seguintes grupos*

$$\mathbb{Z}/n\mathbb{Z} \qquad 1 \leq n \leq 10 \quad ou \quad n = 12$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \qquad 1 \leq n \leq 4$$

Além disso, existe para cada grupo acima uma curva elíptica com este grupo de torção.
Prova: [MAZUR]. □

Antes de utilizarmos estes teoremas na determinação do grupo de torção de algumas curvas, vejamos como se comportam os pontos de 2-torção e 3-torção.

Um ponto não nulo $P = (x, y) \in E(\mathbb{Q})$ é de 2-torção se, e somente se, $P = -P$. Entretanto, vimos (**3.3.6**, pg. 68) que $-P = (x, -y)$; logo um ponto $P = (x, y)$ será de 2-torção se, e só se, $y = 0$. Isto implica que x será então raíz da equação

$$x^3 + ax + b = 0$$

Logo $\#E[2] = 1$ ou $\#E[2] = 2$ ou $\#E[2] = 4$.

Os pontos de 3-torção satisfazem $P + P + P = O$ e como vimos três pontos quaisquer de uma curva elíptica somam para O se, e somente se, estão todos sobre uma reta. Isto nos diz que os pontos de 3-torção são todos aqueles com tangente inflexional. É fácil mostrar, usando a Hessiana de uma curva, que numa cúbica existem no máximo nove pontos de inflexão, ou seja, $\#E[3] \leq 9$.

Importante também na determinação dos pontos de torção é analisar a estrutura "local" de uma curva elíptica, quero dizer, como se comporta E quando definida sobre os diversos corpos $\mathbb{F}_p$, para todo primo p. As informações locais quando "conectadas" revelam fatos importantes: é por exemplo através dos mapas de redução sobre $\mathbb{Z}_p$ que o teorema de Nagell-Lutz é obtido.

Fixemos um primo p e consideremos $E \subset \mathbb{P}^2_{\mathbb{Q}}$ como sendo uma curva elíptica definida sobre $\mathbb{Q}$ de equação de Weierstrass

$$Y^2Z = X^3 + aXZ^2 + bZ^3, \qquad a, b \in \mathbb{Z}$$

Observemos que todo ponto de $(a : b : c) \in \mathbb{P}^2_{\mathbb{Q}}$ podemos supor ser da forma

$$a, b, c \in \mathbb{Z} \qquad \text{e} \qquad \text{mdc}(a, b, c) = 1$$

Logo faz sentido considerarmos o mapa

$$\begin{array}{ccc} \Psi_p : \mathbb{P}^2_{\mathbb{Q}} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ (a : b : c :) & \longmapsto & (\bar{a} : \bar{b} : \bar{c}) \end{array}$$

onde a barra denota a redução módulo p. Chamaremos este mapa de *redução módulo* p. Seja $\bar{E}$ a curva sobre $\mathbb{Z}/p\mathbb{Z}$ dada pela equação

$$Y^2Z = X^3 + \bar{a}XZ^2 + \bar{b}Z^3$$

Note que $\bar{E}$ nem sempre representa uma curva elíptica, pois a redução módulo p pode anular o discriminante tornando a nova curva singular. Exemplo disso é a curva $E : Y^2Z = X^3 + 3Z^3$ que reduzida módulo 3 torna-se a curva singular $\bar{E} : Y^2Z = X^3$. Observemos também que $\Psi_p|E$ define um mapa entre as duas curvas E e $\bar{E}$. De fato, se $P = (a : b : c) \in E(\mathbb{Q})$ então $\Psi_p(P) = (\bar{a} : \bar{b} : \bar{c}) \in \bar{E}(\mathbb{Z}/\mathbb{Z})$. Será este mapa um homomorfismo de grupos? A resposta é sim para infinitos primos. Sim para todos aqueles cuja a redução de E, $\bar{E}$, seja ainda uma curva lisa.

Teorema 6.1.3 *Seja $E/\mathbb{Q}$ uma curva elíptica com equação de Weierstrass $y^2 = x^3 + ax + b$, $a, b \in \mathbb{Z}$ e discriminante Δ. Então o mapa de redução módulo p*

$$\begin{array}{ccc} \Psi_p : E & \longrightarrow & \bar{E} \\ (a : b : c) & \longmapsto & (\bar{a} : \bar{b} : \bar{c}) \end{array}$$

é um homomorfismo de grupos, se $p \nmid \Delta$.

Prova: A adição numa curva elíptica é caracterizada pela seguinte condição:

$$A + B + C = O \Longleftrightarrow A, B \text{ e } C \text{ estão sobre uma mesma reta } L$$

onde A, B e C são pontos de uma curva elíptica. Devemos mostrar então que se $\{A, B, C\} = E \cap L$ então $\{\bar{A}, \bar{B}, \bar{C}\} = \bar{E} \cap \bar{L}$. Para tanto usaremos a seguinte

afirmação
AFIRMAÇÃO : Nestas condições vale: $\{\bar{A}, \bar{B}, \bar{C}\} = \bar{E} \cap \bar{L}$ ou $\bar{L}$ é uma componente irredutível de $\bar{E}$.

Fica portanto clara a demonstração, uma vez que a condição $p \nmid \Delta$ implica justamente que $\bar{E}$ é lisa, logo não contém componentes irredutíveis próprias. □

Lema 6.1.4 *Se $E/\mathbb{Q}$ é uma curva elíptica e $L \subset \mathbb{P}^2_{\mathbb{Q}}$ uma reta definida sobre $\mathbb{Q}$ (logo com coeficientes em $\mathbb{Z}$). Se $\{P_1, P_2, P_3\} = E \cap L$ e $\bar{P}_i$, $\bar{L}$ e $\bar{E}$ representam as respectivas reduções módulo p, então ou $\bar{E}$ e $\bar{L}$ se interceptam em $\bar{P}_i$ ou $\bar{L}$ é uma componente de $\bar{E}$.*
Prova: Mediante uma projetividade ω podemos supor que L é a reta $X = 0$. Seja $g(X, Y, Z)$ o polinômio obtido a partir de $Y^2Z = X^3 + aXZ^2 + bZ^3$ mediante a projetividade ω. Sem perda de generalidade, podemos supor que os coeficientes de g não possuem fatores comuns.

Suponhamos que $P_i(0 : b_i : c_i)$, $\text{mdc}(b_i, c_i) = 1$, sejam os pontos de interseção de E e L. Em outras palavras temos que b_i e c_i são soluções da equação

$$g(0, Y, Z) = 0$$

Se $\bar{g}(0, Y, Z) \equiv 0$ então claramente $\bar{g}(X, Y, Z) = X \cdot \bar{f}(X, Y, Z)$, isto é, a reta $\bar{L}$ é uma componente de E. Do contrário temos que p não divide todos os coeficientes de $g(0, X, Y)$. Daí, por g ter grau três e pela fatoração única de polinômios, segue que

$$g(0, Y, Z) = k(b_1Z - c_1Y)(b_2Z - c_2Y)(b_3Z - c_3Y)$$

para alguma constante k não divisível por p. Logo

$$\bar{G}(0, Y, Z) = \bar{k}(\bar{b_1}Z - \bar{c_1}Y)(\bar{b_2}Z - \bar{c_2}Y)(\bar{b_3}Z - \bar{c_3}Y)$$

e claramente $\bar{P}_i = (0 : \bar{b_i} : \bar{c_i})$ estão na interseção de $\bar{L}$ e $\bar{E}$. □

Ao restringirmos o mapa Ψ_p ao subgrupo $E(\mathbb{Q})_{tors}$ obteremos homomorfismo de grupos, para todo primo $p \nmid \Delta$. Pelo Nagell-Lutz (**6.1.1**, pg. 139), para um ponto não nulo $(a : b : 1) \in E(\mathbb{Q})$ ser de torção é necessário que $a, b \in \mathbb{Z}$. Logo a imagem deste ponto pelo mapa de redução será $\bar{P} = (\bar{a} : \bar{b} : 1)$. Claramente $\bar{P} \neq \bar{O}$, o que implica que o mapa é injetivo. Donde conclui-se

Teorema 6.1.5 *Sejam $E/\mathbb{Q}$ com equação de Weierstrass $y^2 = x^3+ax+b$, $a, b \in \mathbb{Z}$. Se $p \nmid \Delta$ então $E(\mathbb{Q})_{tors}$ é isomorfo a um subgrupo de $\bar{E}(\mathbb{Z}/p\mathbb{Z})$.* □

Corolário 6.1.6 *Seja $r_i = \#\bar{E}(\mathbb{Z}/p_i\mathbb{Z})$, com $p_i \nmid \Delta$, para $i = 1, 2$. Se* $\mathrm{mdc}(r_1, r_2) = 1$ *então $E(\mathbb{Q})_{tors}$ é trivial.*
Prova: O teorema anterior nos diz que $\#E(\mathbb{Q})_{tors}$ divide r_1 e r_2 de onde segue o corolário □

6.2 Exemplos

Vejamos como determinar o subgrupo de torção de algumas curvas elípticas. Para isso usaremos o seguinte algoritmo baseado nos teoremas anteriores:

Passo 1 Seja E dada pela equação de Weierstrass

$$E : Y^3 + a_1XY + a_2Y - X^3 - a_2X^2 - a_4X - a_6 = 0$$

que se transforma numa equação do tipo

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}$$

completando-se o quadrado no primeiro membro, o cubo no segundo e depois racionalizando-se os coeficientes, vide (**3.1**, pg. 56).

Passo 2 Calcula-se o discriminante $\Delta = -16(4a^3 + 27b^2)$.

Passo 3 Encontra-se os divisores y de $\Delta/(-16)$ que satisfazem $y^2|\Delta/(-16)$.

Passo 4 Seleciona-se, se houver, as raízes inteiras da equação (em x) $x^3+ax+b = y^2$.

Passo 5 Calcula-se $[i]P$, $i = 2, 3, ..., e_p$, onde $P = (x, y)$ e $e_p = \#\bar{E}_p(\mathbb{Z}/p\mathbb{Z})$ com p o menor número primo que não divide Δ.

Passo 6 Se alguma dessas potências de P tiverem os coeficientes fracionários, então P não é ponto de torção.

Este algoritmo calcula todos os pontos $P \neq O$ de torção em E e é bastante simples de se implementar. Os exemplos que se seguem foram todos calculados a partir de uma implementação deste algoritmo feito no programa **Maple**:

```
> a1:=1:
> a3:=1:
> a2:=1:
> a4:=1:
> a6:=1:
> print(y^2+a1*xy+a3*y=x^3+a2*x^2+a4*x+a6);
> b2:=a1^2+4*a2:
> b4:=a1*a3+2*a4:
> b6:=a3^2+4*a6:
> c4:=b2^2-24*b4:
> c6:=-b2^3+36*b2*b4-216*b6:
> if a1<>0 or a3<>0 then
> a:=-27*c4:
> b:=-54*c6:
> else;
>    if a2=0 then
>    a:=a4;
>    b:=a6;
>    else;
>    a:=3^3*(3*a4-a2^2);
>    b:=3^5*(3*a6-a4*a2);
>    end if:
> end if:
> print(y^2=x^3+a*x+b);
> d:=-16*(4*a^3+27*b^2);
> Delta:=ifactor(-16*(4*a^3+27*b^2));
> p:=0:
> w:=factorset(d):
> pri:=seq(nextprime(i),i=w):
> for z in pri while p=0 do
> if modp(d,z)<>0 then p:= z end if;
> end do;
> "Primo"=p;
> ap:=modp(a,p):
> bp:=modp(b,p):
```

```
> print(E[p],y^2=x^3+ap*x+bp);
> \Delta[p]:=modp(d,p);
> with(numtheory):
> ep:=1:
> l:=0:
> for i from 0 to p-1 do
> y[i]:=modp(i^3+ap*i+bp,p):
> if quadres(y[i],p)=1  and y[i]<>0 then
> ep:=ep+2
> elif y[i]=0 then ep:=ep+1
> end if;
> end do:
> ep:=ep;
> 0;
> for j from 0 to p-1 do
> if quadres(y[j],p)=1 then t[j]:=Sim else t[j]:=No end if;
> if t[j]=Sim then
> l:=l+1:
> print(Q[l]=[j,msqrt(y[j],p)]);
> if y[j]<> 0  then l:=l+1: print(Q[l]=[j,-msqrt(y[j],p)]) end if:
>  end if;
> end do;
> r[1]:=array(1..2):
> ordem:=ep:
> h:=divisors(d/(-16)):
> zer:=solve(x^3+a*x+b=0,x):
> for as from 1 to 3 do
> if type(zer[as], integer) then
> print(S,[zer[as],0]);
> print([2]*S,0);
> end if;
> end do:
> for u from 1 to tau(d/(-16)) do
> if modp(d,h[u]^2)=0 then
> r[1][2]:=h[u];
> sol:=solve(x^3+a*x+b=r[1][2]^2,x);
> for z from 1 to 3 do
> if type(sol[z], integer) then
> r[1][1]:=sol[z]:
```

```
> r[2]:=array(1..2):
> r[2][1]:=(r[1][1]^4-2*a*r[1][1]^2-
- 8*b*r[1][1]+a^2)/(4*(r[1][1]^3+a*r[1][1]+b)):
> r[2][2]:=-(r[2][1]*(3*r[1][1]^2+a)/(2*r[1][2])+
+ ((-r[1][1]^3+a*r[1][1]+2*b)/(2*r[1][2]))):
> print(S,r[1]);
> print([2]*S , r[2]);
> if (r[2][1]=r[1][1] and r[2][2]=-r[1][2]) then
> print([3]*S, 0);
> else
> for k from 3 to ordem do
> r[k]:=array(1..2):
> r[k][1]:=((r[k-1][2]-r[1][2])/(r[k-1][1]-r[1][1]))^2 -
-(r[k-1][1]+r[1][1]):
> r[k][2]:=-((r[k-1][2]-r[1][2])/(r[k-1][1]-r[1][1]))*r[k][1]+
+ (r[1][2]*r[k-1][1]-r[k-1][2]*r[1][1])/(-r[k-1][1]+r[1][1]):
> if not type(r[2][1],fraction) then
> print([k]*S, r[k]);
> if type(r[k][1],fraction) then
> k:=ordem:
> print(r[1],"nao 'e de Torsao");
> end if:
> if (r[k][1]=r[1][1] and r[k][2]=-r[1][2]) then
> print([k+1]*S, 0);
> k:=ordem:
> end if;
> else
> k:=ordem:
> print(r[1],"nao 'e de Torsao");
> end if;
> end do;
> end if;
> else
> end if;
> end do;
> end if;
> end do;
```

Exemplo 6.1 $y^2 = x^3 - 432x + 8208$.

$$\Delta = -2^{12} \cdot 3^{12} \cdot 11$$
$$\bar{E}_5 : y^2 = x^3 - 2x + 3$$

Consideremos a curva E reduzida módulo 5, $\bar{E}_5$. Como $5 \nmid \Delta$ temos que $E(\mathbb{Q})_{tors} \subset \bar{E}_5(\mathbb{Z}/5\mathbb{Z})$. Observemos que

$$\bar{E}_5(\mathbb{Z}/5\mathbb{Z}) = \{O, (3,2), (3,3), (4,2), (4,4)\}$$

ou seja, a ordem de $E(\mathbb{Q})_{tors}$ ou é 1 ou é 5. Caso ele possua algum ponto de torção não nulo, teremos que $E(\mathbb{Q})_{tors} \equiv \mathbb{Z}/5\mathbb{Z}$. Claramente E não pode ter pontos de 2-torção, logo $b \neq 0$ para $(a,b) \in E(\mathbb{Q})_{tors}$. Desta forma devemos ter $b^2 \mid \Delta$. Alguns cálculos nos dizem que o ponto $R = (12, 108) \in E$ pode ser um ponto de torção. E de fato é, pois $[5]R = O$.

Exemplo 6.2 $E(\mathbb{Q})_{tors}$ *é trivial.*

$$E : y^2 = x^3 + 32x + 16$$
$$\Delta = -2^{12} \cdot 7^2 \cdot 11$$

Temos que

$$\bar{E}_3(\mathbb{Z}/3\mathbb{Z}) = \{O, (0,1), (0,-1), (1,1), (1,-1), (2,1), (2,-1)\}$$

e portanto $\#\bar{E}_3(\mathbb{Z}/3\mathbb{Z}) = 7$, enquanto que $\#\bar{E}_{13}(\mathbb{Z}/13\mathbb{Z}) = 18$. Portanto pelo corolário (**6.1.6**, pg. 143) temos que $E(\mathbb{Q})_{tors}$ é trivial.

Usando o Nagell-Lutz (**6.1.1**, pg. 139) podemos chegar ao mesmo resultado. Consideremos os possíveis pontos de torção(aqueles cuja coordenada y satisfaz $y^2|(2^8 \cdot 7^2 \cdot 11)$). Simples cálculos nos mostram que $P_1 = (0,4)$, $P_2 = (1,7)$ e $P_3 = (8,28)$ são os possíveis pontos de torção. No entanto temos

$$[3]P_1 = (\frac{17}{4}, \frac{121}{8})$$
$$[2]P_2 = (\frac{17}{4}, \frac{121}{8})$$

$$[6]P_3 = (\frac{17}{4}, \frac{121}{8})$$

ou seja, o único ponto de torção é O.

Exemplo 6.3 $E' : y^2 + xy - 5y = x^3 - 5x^2$.

Esta curva está na classe de isomorfismo da curva

$$E : y^2 = x^3 - 12987x - 263466$$

e para esta curva temos

$$\Delta = 2^{12} \cdot 3^{16} \cdot 5^4$$

Além disso

$$\bar{E}_3(\mathbb{Z}/3\mathbb{Z}) = \{O, (0,0), (2,2), (2,-2), (3,0), (4,0), (6,1), (6,-1)\}$$

Como $x^3 - 12987x - 263466 = (x+21)(x+102)(x-123)$, os pontos de 2-torção são $(-21, 0)$, $(-102, 0)$ e $(123, 0)$. Pelo Nagell-Lutz os possíveis pontos de torção (x, y), com $y \neq 0$, são

$$P = (-57, 540) \qquad \text{e} \qquad Q = (303, 4860)$$

Entretanto $[3]P = -P$ e $[3]Q = -Q$. Logo,

$$E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

Exemplo 6.4 $E_{(n)} : y^2 = x^3 - n^2x = x(x-n)(x+n)$.

$$\Delta_n = (2n)^6$$

Mostraremos que

$$E_{(n)}(\mathbb{Q})_{tors} = \{O, (0,0), (n,0), (-n,0)\} = E_{(n)}[2] \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$$

todos de ordem 2. Usaremos para tanto o belíssimo teorema de Dirichlet sobre primos em progressão aritmética

Teorema 6.2.1 (Dirichlet) *Sejam a e b inteiros co-primos. Então existem infinitos primos da forma*

$$an + b, \qquad n \in \mathbb{N}$$

Prova: [ROSE] □

Suponhamos por absurdo que $E_{(n)}$ possua um ponto não nulo de ordem finita maior que 2. Então $E_{(n)}(\mathbb{Q})_{tors}$ contém um elemento de ordem ímpar ou o subgrupo formado pelos pontos de ordem 4 contém 8 ou 16 elementos. Em qualquer dos casos existe um subgrupo $S \subset E_{(n)}(\mathbb{Q})_{tors}$ com m elementos, onde m é igual a 8 ou um inteiro ímpar. E como para todo primo $p \nmid 2n$ obtemos

$$E_{(n)}(\mathbb{Q})_{tors} \subset \bar{E}_{(n)}(\mathbb{Z}/p\mathbb{Z})$$

vemos, por (**4.2**, pg. 102), que m divide $p + 1$ sempre que $p \equiv 3 \mod 4$. Em outras palavras, existe apenas um número finito de primos (aqueles que dividem $2n$) satisfazendo

$$(*) \begin{cases} p \not\equiv -1 \mod m \\ p \equiv 3 \mod 4 \end{cases}$$

Entretanto para $m = 8$ conseguimos (Dirichlet) infinitos primos p da forma $8k+3$ e todos eles satisfazem

$$\begin{cases} p \equiv 3 \mod 8 \\ p \equiv 3 \mod 4 \end{cases}$$

contrariando a finitude das soluções de $(*)$.

Caso m seja um número ímpar não divisível por 3, a infinitude de primos em $4mk + 3$ produz infinitas soluções para $(*)$.

Caso $3|m$, basta considerar a progressão aritmética $12k + 7$ que pelos mesmos motivos leva a uma contradição. Logo, como queríamos demonstrar,

$$\#E_{(n)}(\mathbb{Q})_{tors} = 4$$

6.3 Conjecturas de Birch e Swinnerton-Dyer

Enfim vimos, nas seções anteriores, como determinar plenamente a estrutura de $E(\mathbb{Q})_{tors}$ para uma curva elíptica E. Para o posto de uma curva elíptica, entretanto,

não há nenhum resultado que permita calculá-lo ou ao menos mostrar que existam curvas elípticas com posto arbitrariamente grande; pelo contrário, os principais exemplos conhecidos possuem todos postos pequenos (entre 7 e 15). Atualmente, os principais problemas em aberto sobre curvas elípticas, incluindo as conjecturas do título, tratam deste número. Entre 1950 e 1960, Birch e Swinnerton-Dyer, baseados em extensiva evidência numérica obtida a partir de computadores, proporam algumas conjecturas que seriam o análogo para curvas elípticas do Princípio Local-Global das Cônicas. A idéia que eles tiveram foi que quanto maior for $E(\mathbb{Q})$ (o que pode ser medido através do posto de E) maior deverá ser $E(\mathbb{F}_p)$, para todo primo p (e isto é medido por $\#E(\mathbb{F}_p)$). O que fizeram foi concatenar os vários valores de $N_p = \#E(\mathbb{F}_p)$ numa única função: a *L-função de Hasse-Weil de E* definida por

$$L(E,s) = \prod_{p\nmid\Delta}(1 - \frac{1+p-N_p}{p^s} + \frac{p}{p^{2s}})^{-1} \times \prod_{p|\Delta} \ell_p(E,s)^{-1}$$

onde Δ é o discriminante de $E : y^2 = x^3 + ax + b$, $\ell_p(E,s)$ é um certo polinômio em p^{-s} tal que $\ell_p(E,1) \neq 0$ e s é uma variável complexa.

Notemos que a cota de Hasse (**4.2.2**, pg. 95) nos diz que esta série converge absolutamente quando $\mathbf{Re}(s) > 3/2$. A partir de um resultado demonstrado por Wiles (o mesmo do Teorema de Fermat), Breuil, Conrad, Diamond e Taylor demonstraram a conjectura de Shimura-Taniyama que implica que

Teorema 6.3.1 (Conjectura de Hasse-Weil) *Seja $E/\mathbb{Q}$ uma curva elíptica. Então $L(E,s)$ possui uma continuação analítica para o plano complexo $\mathbb{C}$.*

Prova: Veja [RUBIN-SILVEBERG], pg. 461, para maiores referências. □

Logo faz sentido calcular $L(E,1)$.

Sendo assim o que Birch e Swinnerton-Dyer propuseram foi que a ordem deste zero, $s = 1$, é o posto da curva elíptica E.

Conjectura 6.3.1 (BSD I) *Seja $E/\mathbb{Q}$ uma curva elíptica. Considere a expansão de Taylor de $L(E,s)$ em torno de $s = 1$, isto é,*

$$L(E,s) = b_r(s-1)^r + b_{r+1}(s-1)^{r+1} + ...$$

com $b_r \in \mathbb{C}\backslash\{0\}$ e r um inteiro não negativo. Então r é o posto de E.

Se esta conjectura for verdadeira teremos uma maneira efetiva de calcular o posto de uma curva elíptica. Infelizmente, apesar do esforço de vários matemáticos brilhantes, o BSD I parece estar longe de ser demonstrado.

Capítulo 7

Aplicações a Teoria dos Números

7.1 Pitágoras, Diofanto e Fermat

Para os matemáticos o teorema de Fermat é certamente um dos mais famosos resultados da Matemática. Enquanto que para a maioria daqueles que não se dedicam com um certo afinco a Matemática, se perguntarmos o nome de algum teorema, a primeira (e talvez única resposta) será: "Teorema de Pitágoras". Talvez porque as aplicações deste teorema a Geometria sejam inúmeras ou por ser sua demonstração e enunciado bastante simples. Este teorema garante que

> *Em um triângulo retângulo o quadrado da hipotenusa é igual a soma do quadrado dos catetos.*

Em outras palavras, as medidas dos lados de um triângulo retângulo satisfazem a *equação de Pitágoras*

$$X^2 + Y^2 = Z^2.$$

Foi Diofanto que em seu livro se propôs a descobrir triângulos retângulos com lados de medidas inteiras ou racionais, isto é, soluções inteiras ou racionais para a equação de Pitágoras. Neste seu livro ele determina uma maneira de obter todas as soluções (inteiras ou racionais) para a equação de Pitágoras. Antes de demonstrarmos o resultado de Diofanto, façamos algumas definições.

Uma solução (x, y, z) com $0 < x < y < z$ para equação de Pitágoras será chamada de *tripla ou terna pitagórica*. Se uma terna pitagórica (x, y, z) é tal que

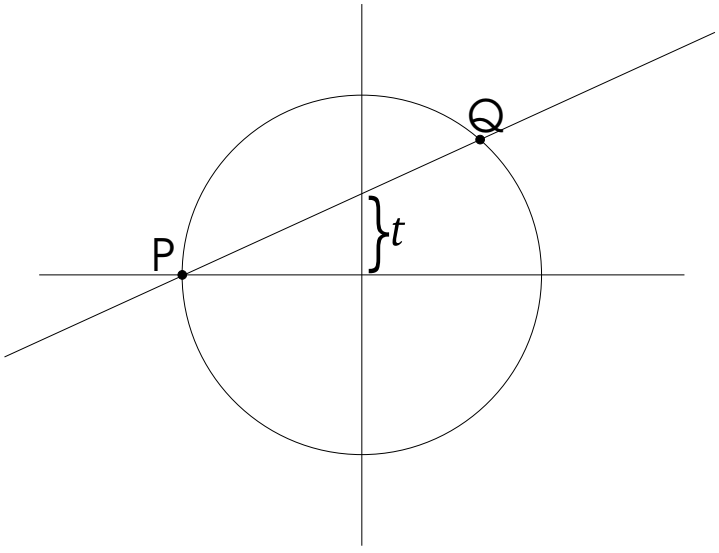
$\text{mdc}(x, y, z) = 1$ diremos que ela é *primitiva*. Toda terna pitagórica é obtida a partir de uma terna pitagórica primitiva, já que $(\lambda x, \lambda y, \lambda z)$, $\lambda \neq 0$, é uma solução se, e somente se, (x, y, z) é uma terna pitagórica. Diante disto temos

Teorema 7.1.1 *(a, b, c) é uma tripla pitagórica primitiva se, e somente se, existirem inteiros m, n relativamente primos tais que $a = m^2 - n^2$, $b = 2mn$ e $c = m^2 + n^2$.*

Prova: Se $a = m^2 - n^2$, $b = 2mn$ e $c = m^2 + n^2$, com $\text{mdc}(m, n) = 1$ então claramente (a, b, c) é um terno pitagórico primitivo. Para a recíproca, vejamos duas demonstrações diferentes: uma baseada no fato de toda cônica ser uma curva racional e a outra totalmente aritmética.

(Geométrica) Uma solução inteira para $X^2 + Y^2 = Z^2$, com $Z \neq 0$ dá origem a um ponto racional na circunferência $x^2 + y^2 = 1$, e vice versa: pontos racionais na circunferência correspondem a uma terna pitagórica.

Uma reta com inclinação racional t e passando por $P = (-1, 0)$ toca a circunferência num ponto racional. Reciprocamente, se Q é um ponto racional da circunferência, a reta unindo P a Q terá inclinação racional. Notemos que uma reta deste tipo intercepta o eixo y no ponto racional $(0, t)$, onde t é a inclinação desta reta.



Assim a terna pitagórica primitiva (a, b, c) podemos associar um ponto da circunferência $Q = (x, y)$, onde $x = a/c$ e $y = b/c$ são frações irredutíveis. Por sua vez a Q podemos associar um número racional t, que é a inclinação da reta que passa por P e Q. A reta de equação $y = t(x + 1)$ intercepta a circunferência no ponto Q e logo

$$\begin{aligned} x^2 + t^2(x+1)^2 &= 1 \\ (1+t^2)x^2 + 2t^2x + t^2 - 1 &= 0 \\ &\Downarrow \\ x &= \frac{1-t^2}{1+t^2} \\ y &= \frac{2t}{1+t^2} \end{aligned}$$

Se tomarmos a fração irredutível $t = \dfrac{n}{m}$ obtemos

$$\frac{a}{c} = x = \frac{m^2 - n^2}{m^2 + n^2} \qquad \text{e} \qquad \frac{b}{c} = y = \frac{2mn}{m^2 + n^2}.$$

Note que a frações $\dfrac{m^2 - n^2}{m^2 + n^2}$ e $\dfrac{2mn}{m^2 + n^2}$ são irredutíveis, pois caso contrário m e n teriam um fator primo comum. Portanto

$$a = m^2 - n^2 \qquad b = 2mn \qquad c = m^2 + n^2$$

(Aritmética) Seja (a, b, c) um terno pitagórico primitivo. Podemos supor b par e a e c ímpares. Assim

$$b^2 = c^2 - a^2 = (c - a)(c + a).$$

Se p é um fator primo ímpar comum de $(c - a)$ e $(c + a)$ então p divide b e além disso

$$p \mid 2c \qquad \text{e} \qquad p \mid 2a$$

contrariando o fato de (a, b, c) ser primitivo. Portanto existem m e n tais que

$$\frac{c-a}{2} = m^2 \qquad \text{e} \qquad \frac{c+a}{2} = n^2$$

o que demonstra o resultado. □

Foi a margem deste teorema, em sua cópia da *Aritmética* de Diofanto que Fermat enunciou o mais famoso dos comentários

"Ao contrário, é impossível separar um cubo em dois cubos, uma potência quarta em duas potências quartas, ou em geral, qualquer potência acima da segunda em duas potências do mesmo grau. Eu descobri uma demonstração verdadeiramente maravilhosa que esta margem é muito estreita para conter."

Se essa demonstração existiu deve ter sido de fato maravilhosa uma vez que as mentes mais brilhantes da matemática jamais conseguiram reproduzí-la. Conjectura-se que Fermat mais tarde percebeu a falsidade de sua demonstração já que mais adiante, em outra anotação marginal de seu livro, ele fez um esboço da demonstração para $n = 4$. Para $n = 4$ a demonstração é bastante simples e oferece mais um exemplo do método usado por Fermat em suas demonstrações - a descida ao infinito - bem como uma aplicação do teorema anterior caracterizando os ternos pitagóricos primitivos. Na realidade mostraremos algo mais forte:

Teorema 7.1.2 *A equação*

$$X^4 + Y^4 = Z^2$$

não possui soluções inteiras (x, y, z) *com* $xyz \neq 0$.

Prova: Suponhamos por absurdo que $x^4 + y^4 = z^2$ e que $xyz \neq 0$. Podemos supor $x, y, z > 0$ e tomar z mínimo dentre todas as soluções para esta equacão.

Se $x = ax'$ $y = ay'$ e $z = az'$ então temos para algum z_1

$$a^2(x'^4 + y'^4) = z'^2 \Longrightarrow x'^4 + y'^4 = z_1'^2.$$

Neste caso $z > z_1'$ contraria a minimalidade de z. Logo $\text{mdc}(x, y, z) = 1$.

Usamos o teorema anterior (**7.1.1**, pg. 153) com $(x^2)^2+(y^2)^2 = z^2$ para obtermos inteiros m e n relativamente primos tais que

$$x^2 = m^2 - n^2 \qquad y^2 = 2mn \qquad z^2 = m^2 + n^2.$$

Note que $x^2 + n^2 = m^2$ é uma terna primitiva, pois, do contrário, se x, m e n tivessem um fator comum, este automaticamente seria um fator de x, y e z. Assim, mais uma aplicação de (**7.1.1**, pg. 153) nos dá inteiros s e t relativamente primos tais que

$$x = s^2 - t^2 \qquad n = 2st \qquad m = s^2 + t^2.$$

Portanto

$$y^2 = 4st(s^2 + t^2)$$

e como $\text{mdc}(s,t) = 1$ temos que $s = a^2$, $t = b^2$ e $s^2 + t^2 = c^2$. Donde

$$a^4 + b^4 = c^2.$$

Notemos que

$$\begin{aligned} z^2 &= m^2 + n^2 \\ &= 4a^4b^4 + (a^4 + b^4)^2 \\ &> (a^4 + b^4)^2 = c^4 \\ &> c^2 \end{aligned}$$

Contrariando o fato de z ser mínimo dentre todas as soluções. □

Corolário 7.1.3 *A equação*

$$X^4 + Y^4 = Z^2$$

não possui soluções racionais (x, y, z) *com* $xyz \neq 0$.
Prova: Nestas condições uma solução $x = r/s$, $y = u/v$ e $z = a/b$ para esta equação implicaria que

$$b^2((vr)^4 + (su)^4) = (as^2v^2)^2$$

ou seja, existe um inteiro c tal que

$$(vr)^4 + (su)^4 = c^2$$

contradizendo o resultado anterior. □

Corolário 7.1.4 *A equação de Fermat*

$$X^4 + Y^4 = Z^4$$

não possui soluções racionais (x, y, z) *além daquelas com* $xyz = 0$.
Prova: Uma solução (x, y, z), com $xyz \neq 0$, para esta equação de Fermat daria origem a uma solução (x, y, z^2) com $xyz^2 \neq 0$ para a equação considerada anteriormente

$$x^4 + y^4 = (z^2)^2.$$

□

Outro problema que surge a partir da equacão de Pitágoras é a determinação de quais números racionais n correspondem a áreas de triângulos retângulos com lados racionais. Observe que só é necessário considerarmos inteiros n livres de quadrado já que se n é a área de um triângulo retângulo com lados (a, b, c) racionais então m^2n é a área do triângulo (ma, mb, mc). Neste caso n é chamado de *número congruente*.

Este problema recebeu uma considerável atenção dos matemáticos ao longo do tempo: os árabes mostraram que para tal n existe x tal que x, $x + n$ e $x - n$ são quadrados e que o contrário também vale; Euler demonstrou que $n = 7$ é congruente, enquanto que Fermat mostrou que $n = 1$ não é congruente. Outros exemplos de números não congruentes são 1, 2, 3 e 4.

Exemplo 7.1 2 *não é congruente.*

Se 2 fosse congruente existiriam racionais x, y e z tais que

$$\begin{cases} x^2 + y^2 = z^2 \\ \dfrac{xy}{2} = 2 \end{cases}$$

Daí $y = \dfrac{2^2}{x}$, para algum m, e

$$x^4 + 2^4 = (zx)^2.$$

Isto contradiz (**7.1.3**, pg. 156).

Nas próximas seções pretendemos relacionar estes problemas à teoria das Curvas Elípticas de maneira que possamos resolvê-los "satisfatoriamente".

7.2 Números Congruentes

A relação que há entre curvas elípticas e números congruentes é dada pelo seguinte teorema

Teorema 7.2.1 *Para um inteiro n livre de quadrado, os três seguintes conjuntos estão em bijeção:*

1. *Triplas de racionais (a, b, c), $a < b < c$, que são soluções do sistema*

$$\begin{cases} a^2 + b^2 = c^2 \\ \dfrac{ab}{2} = n \end{cases}$$

2. *Números racionais x tais que x, $x + n$ e $x - n$ são quadrados;*

3. *Pontos $(x, y) \in E_{(n)}(\mathbb{Q})$, com $E_{(n)} : Y^2 = X^3 - n^2X$ uma curva elíptica e x o quadrado de um número racional com denominador par.*

Prova: Temos que se (a, b, c) é um terno pitagórico de área n então

$$\left(\frac{a+b}{2}\right)^2 = \frac{a^2 + 2ab + b^2}{4} = \frac{c^2 + 4n}{4} = \left(\frac{c}{2}\right)^2 + n$$

e

$$\left(\frac{a-b}{2}\right)^2 = \left(\frac{c}{2}\right)^2 - n$$

Logo se fizermos $x = (c/2)^2$ então teremos que x, $x + n$ e $x - n$ são quadrados.

Reciprocamente se x, $x + n$ e $x - n$ são quadrados então definimos $c = 2\sqrt{x}$ e tomamos $a < b$ tais que

$$\left(\frac{a \pm b}{2}\right)^2 = \frac{c^2}{4} \pm n.$$

Desta forma (a, b, c) é uma terna pitagórica com $n = \frac{1}{2}ab$.

Para relacionarmos os conjuntos (2) e (3), assumamos inicialmente que x pertence ao conjunto (2), então $x = u^2$ e

$$v^2 = (x - n)(x + n) = x^2 - n^2 = u^4 - n^2$$

que ao multiplicarmos por u^2 torna-se

$$(uv)^2 = u^6 - n^2u^2$$

Façamos $y = uv$ e $x = u^2$ então o ponto (x, y) pertence a cúbica

$$Y^2 = X^3 - n^2X.$$

Usando a bijeção entre (1) e (2) vemos que $x = c^2/4$ tem denominador par.

Por outro lado se x é um quadrado com denominador par, isto é, $x = (c/2)^2$ e se $x^3 - n^2x$ é um quadrado y^2 então pondo $v = y/\sqrt{x}$ obtemos

$$v^2 = \frac{y^2}{x} = \frac{x^3 - n^2x}{x} = x^2 - n^2.$$

Isto é

$$v^2 + n^2 = x^2$$

é um terno pitagórico. Como n é inteiro temos que os denominadores de x^2 e v^2 são iguais; digamos t^4 com t divisível por 2, por hipotése. Portanto a tripla pitagórica

$$(t^2v)^2 + (t^2n)^2 = (t^2x)^2$$

é primitiva, e por (**7.1.1**, pg. 153), deve ser da forma

$$t^2v = M^2 - N^2 \qquad t^2n = 2MN \qquad t^2x = M^2 + N^2$$

Ao multiplicarmos a tripla pitagórica $t^2x = M^2 + N^2$ por $4/t^2$ obtemos uma outra terna pitagórica

$$\Big(\frac{2M}{t}\Big)^2 + \Big(\frac{2N}{t}\Big)^2 = 4x$$

que determina um triângulo retângulo de área

$$\frac{4MN}{2t^2} = \frac{t^2n}{t^2} = n.$$

Isto estabelece a equivalência entre os três conjuntos. □

O próximo resultado caracteriza os números congruentes n em termos de propriedades da curva elíptica $E_{(n)}$.

Corolário 7.2.2 *n é congruente se, e só se, $E_{(n)}(\mathbb{Q})$ tem posto não nulo.*
Prova: Se n é congruente então por (**7.2.1**, pg. 157) existe um ponto $(x, y) \in E_{(n)}(\mathbb{Q})$ com x um quadrado racional de denominador par. Logo, pelo Nagell-Lutz (**6.1.1**, pg. 139), este ponto (x, y) não pode ser de torção, pois suas coordenadas não são inteiras. Portanto tem ordem infinita.

Reciprocamente, se $E_{(n)}(\mathbb{Q})$ tem um ponto de ordem infinita (x, y) então $[2](x, y) = (x', y') \neq O$. Uma aplicação da fórmula da duplicação (**3.3.6**, pg. 68) nos diz que

$$x' = \frac{x^4 + 2n^2x^2 + n^4}{4(x^3 - n^2x)} = \Big(\frac{x^2 + n^2}{2y}\Big)^2$$

Logo $[2](x,y)$ é um ponto cuja coordenada x' é um quadrado com denominador par e por (**7.2.1**, pg. 157) corresponde a uma tripla pitagórica (a,b,c) cuja área é n, isto é, n é um número congruente. □

De posse deste corolário e do exemplo (**7.1**, pg. 157) da seção anterior vemos que a curva elíptica $E_{(2)}$ tem posto nulo, ou melhor, $\#E_{(2)}(\mathbb{Q}) < \infty$. Assim, por (**6.4**, pg. 148), a curva $E_{(2)}$ dada por $Y^2 = X^3 - 4X$ satisfaz

$$E_{(2)}(\mathbb{Q}) = \{O, (0,0), (2,0), (-2,0)\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Como 6 é a área do triângulo de lados $(3,4,5)$ vemos que a curva dada por $E_{(6)}$ tem posto ≥ 1.

Logo uma maneira efetiva de calcular o posto de uma curva elíptica permitiria dizer quando um número é ou não congruente. Infelizmente, como observamos anteriormente, não existe ainda uma maneira de determinarmos o posto de uma curva elíptica. As conjecturas de Birch e Swinnerton-Dyer se verdadeiras para as curvas $E_{(n)}$ implicam o seguinte critério descoberto por J. Tunnell

Teorema 7.2.3 (Tunnell) *Seja n um inteiro livre de quadrados e $1 \leq a \leq 2$ satisfazendo $n \equiv a \mod 2$. Então n é congruente se, e somente se,*

$$\#\{(x,y,z) \in \mathbb{Z}^3 \mid \frac{n}{a} = 2ax^2 + y^2 + 32z^2\} = \frac{1}{2}\#\{(x,y,z) \in \mathbb{Z}^3 \mid \frac{n}{a} = 2ax^2 + y^2 + 8z^2\}$$

Prova: [KOBLITZ], pg. 221 □

Para maiores informações sobre este problema veja o excelente livro de [KOBLITZ] ou o artigo original de [TUNNELL].

7.3 O Último teorema de Fermat

O último Teorema de Fermat resistiu a várias tentativas, mas finalmente sucumbiu ao ser relacionado com a teoria de curvas elípticas e formas modulares. Infelizmente, a idéia envolve muitas ferramentas avançadas que não pretendemos reproduzir aqui; pelo contrário o seguinte "esboço" da demonstração carece de rigor matemárico, sendo somente uma maneira de aguçar a curiosidade do leitor e apontar outras

referências. Para se ter uma idéia da dificuldade, a demontração de Wiles é um artigo com quase 200 páginas!!

A idéia original partiu de Gerhart Frey (1985) que estudava as curvas elípticas do tipo

$$Y^2 = X(X - A)(X - B), \text{ com } A + B = C.$$

Ele pôs $A = a^p$ e $B = b^p$, onde $p \geq 5$ é um primo e (a, b, c), $abc \neq 0$, é uma solução hipotética para a equação de Fermat

$$X^p + Y^p = Z^p.$$

Frey observou que se existisse tal curva, ela possuíria propriedades contrastantes com as de outras curvas elípticas. Ele ficou convencido de que tal situação era impossível e pensou num método para derivar uma contradição com a bem conhecida conjectura de Shimura-Taniyama. Esta conjectura (atualmente um teorema provado recentemente por Breuil, Conrad, Diamond e Taylor e obtido como uma extensão do trabalho de Wiles) relaciona curvas elípticas e formas modulares

Teorema 7.3.1 (Conjectura de Shimura-Taniyama) *Toda curva elíptica definida sobre $\mathbb{Q}$ é modular.*

De uma maneira não muito precisa, uma curva elíptica E é modular se existir uma função modular f tal que a L-série associada a E é igual a L-série associada a f (isto não é uma definição).

Ken Ribet em 1986 provou uma conjectura de Serre (*a conjectura epsilon*) que automaticamente acarretava que a validade da conjectura de Shimura-Taniyama implicaria o Último teorema de Fermat. Restava apenas demonstrar esta conjectura.

Finalmente, em 1993, após vários anos "enclausurado" em seu sótão, Andrew Wiles anunciou uma prova para a conjectura de Shimura-Taniyama para um grupo muito especial de curvas elípticas, das quais a curva de Frey fazia parte. Infelizmente esta continha ainda algumas falhas, que puderam ser sanadas um ano depois com a ajuda de Richard Taylor.

Para afirmações precisas recomendamos o primeiro capítulo de [CORNELL-SILVERMAN-STEVENS] ou ainda o livro de [RIBENBOIM]. Para uma abordagem sobre o Último Teorema de Fermat mais histórica e menos matemática recomendamos [SINGH], cuja apresentação não requer nenhum conhecimento de matemática, além de ser uma leitura excepcional.

Bibliografia

[BRESSOUD] Bressoud, David M., *Factorization and Primality Testing*, Springer, **1989**.

[BOREVICH-SHAFAREVICH] Borevich, Z. I. & Shafarevich, I. R., *Number Theory*, Academic Press, **1966**.

[CASSELS] Cassels, J. W. S., *Lectures on Elliptic Curves*, Cambridge University Press, **1991**.

[CASSELS2] _____, Mordell's finite basis theorem revisited, *Math. Proc. Cambridge Philosophical Soc.*, **100**, 31-41(1986).

[CORNELL-SILVERMAN-STEVENS] Cornell, G. & Silverman, J.H. & Stevens, G.(Editores), *Modular Forms and Fermat's Last Theorem*, Springer-Verlag, **1997**.

[FULTON] Fulton, Willliam, *Algebraic Curves*, Benjamin, **1969**.

[FULTON2] _____, *Algebraic Topology*, Springer, **1995**.

[GOUVÊA] Gouvêa, Fernando Q., *P-adic numbers*, Springer-Verlag, **1993**.

[HARTSHORNE] Hartshorne, R., *Algebraic Geometry*, Springer-Verlag, **1977**.

[HINDRY-SILVERMAN] Hindry, Marc & Silverman, Joseph H., *Diophantine Geometry*, Springer, **2000**.

[HUSEMÖLLER] Husemöller, Dale, *Elliptic Curves*, Springer-Verlag, **1987**.

[KOBLITZ] Koblitz, N., *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, **1984**.

[MATSUMURA] Matsumura, H., *Commutative Ring Theory*, Cambridge University Press, **1986**.

[MAZUR] Mazur, B. Rational Points on modular curves, *Modular functions in one Variable V*, Lectures Notes 601. pp. 107-148. Springer, **1977**.

[MORDELL] Mordell, L. J., On the rational Solutions of the indeterminate equations of the third and fourth degrees, *Proc. Camb. Phil. Soc.*, **21**, 179-192(1922).

[MORDELL2] _____, *Diophantine Equations*, Academic Press, **1969**.

[RIBENBOIM] Ribenboim, Paulo, *Fermat's Last Theorem for amateurs*, Springer-Verlag, **1999**.

[ROSE] Rose, H. E., *A course in Number Theory*, Oxford Science Publications, **1994**.

[RUBIN-SILVEBERG] Rubin, Karl & Silverberg, Alice, Ranks of Elliptic Curves, *Bull. Amer. Math. Soc.*, **39**, 455-474(2002).

[SERRE] Serre, J.-P., *A course in Arithmetic*, Springer-Verlag, **1973**.

[SHAFAREVICH] Shafarevich, I. R., *Basic Algebraic Geometry*, Springer-Verlag, **1977**.

[SILVERMAN] Silverman, Joseph H., *The Arithmetic of Elliptic Curves*, Springer-Verlag, **1986**.

[SILVERMAN2] Silverman, Joseph H., *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, **1994**.

[SILVERMAN-TATE] _____ & Tate, John, *Rational Points on Elliptic Curves*, Springer, **1992**.

[SINGH] Singh, Simon, *O Último Teorema de Fermat*, Ed. Record, **1999**.

[TUNNELL] Tunnell, J., A classical Diophantine problem and modular forms of weight 3/2, *Inventiones Math.*, **72**, 323-334(1983).